THE FUTURE OF MONEY—PART 1

HEARING

BEFORE THE

SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL MONETARY POLICY

OF THE

COMMITTEE ON BANKING AND FINANCIAL SERVICES

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

JULY 25, 1995

Printed for the use of the Committee on Banking and Financial Services

Serial No. 104–27

U.S. GOVERNMENT PRINTING OFFICE

92–489 CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052055-X

THE FUTURE OF MONEY—PART 1

HEARING

BEFORE THE

SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL MONETARY POLICY

OF THE

COMMITTEE ON BANKING AND FINANCIAL SERVICES

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

JULY 25, 1995

Printed for the use of the Committee on Banking and Financial Services

Serial No. 104-27

U.S. GOVERNMENT PRINTING OFFICE

92-489 CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052055-X

HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES

JAMES A. LEACH, Iowa, *Chairman*
BILL McCOLLUM, Florida, *Vice Chairman*

MARGE ROUKEMA, New Jersey
DOUG BEREUTER, Nebraska
TOBY ROTH, Wisconsin
RICHARD H. BAKER, Louisiana
RICK LAZIO, New York
SPENCER BACHUS, Alabama
MICHAEL CASTLE, Delaware
PETER KING, New York
EDWARD ROYCE, California
FRANK D. LUCAS, Oklahoma
JERRY WELLER, Illinois
J.D. HAYWORTH, Arizona
JACK METCALF, Washington
SONNY BONO, California
ROBERT NEY, Ohio
ROBERT L. EHRLICH, Maryland
BOB BARR, Georgia
DICK CHRYSLER, Michigan
FRANK CREMEANS, Ohio
JON FOX, Pennsylvania
FREDERICK HEINEMAN, North Carolina
STEVE STOCKMAN, Texas
FRANK LoBIONDO, New Jersey
J.C. WATTS, Oklahoma
SUE W. KELLY, New York

HENRY B. GONZALEZ, Texas
JOHN J. LaFALCE, New York
BRUCE F. VENTO, Minnesota
CHARLES E. SCHUMER, New York
BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
JOSEPH P. KENNEDY II, Massachusetts
FLOYD H. FLAKE, New York
KWEISI MFUME, Maryland
MAXINE WATERS, California
BILL ORTON, Utah
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
LUCILLE ROYBAL-ALLARD, California
THOMAS M. BARRETT, Wisconsin
NYDIA M. VELAZQUEZ, New York
ALBERT R. WYNN, Maryland
CLEO FIELDS, Louisiana
MELVIN WATT, North Carolina
MAURICE HINCHEY, New York
GARY ACKERMAN, New York
KEN BENTSEN, Texas

BERNARD SANDERS, Vermont

SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL MONETARY POLICY

MICHAEL CASTLE, Delaware, *Chairman*
EDWARD ROYCE, California, *Vice Chairman*

FRANK LUCAS, Oklahoma
JACK METCALF, Washington
BOB BARR, Georgia
DICK CHRYSLER, Michigan
FRANK LoBIONDO, New Jersey
J.C. WATTS, Oklahoma
SUE W. KELLY, New York
ROBERT NEY, Ohio
JON FOX, Pennsylvania

FLOYD H. FLAKE, New York
BARNEY FRANK, Massachusetts
JOSEPH P. KENNEDY II, Massachusetts
CAROLYN B. MALONEY, New York
LUCILLE ROYBAL-ALLARD, California
THOMAS M. BARRETT, Wisconsin
CLEO FIELDS, Louisiana
MELVIN WATT, North Carolina

BERNARD SANDERS, Vermont

CONTENTS

THE FUTURE OF MONEY—PART 1

TUESDAY, JULY 25, 1995

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON DOMESTIC AND
INTERNATIONAL MONETARY POLICY,
COMMITTEE ON BANKING AND FINANCIAL SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:02 a.m., in room 2128, Rayburn House Office Building, Hon. Michael N. Castle [chairman of the subcommittee] presiding.

Present: Chairman Castle, Representatives Royce, Lucas, Metcalf, Chrysler, Kelly, Fox, Flake, Maloney, and Watt.

Chairman CASTLE. The subcommittee will come to order. Welcome to the House Banking and Financial Services Committee, Subcommittee on Domestic and International Monetary Policy hearing. That is a very long name. Monetary Policy is probably the correct name. This hearing is on the future of money. Again, this subcommittee is positioned to have initial jurisdiction of an important area of public policy.

Mr. Lucas is here. You do not see other Members, but as I explained to the panelists, Members will come and go during the course of the day. Their staffs are here.

We have your testimony. We look forward to hearing your oral testimony. We will go through each of you, from Mr. Van Lear all the way over to Mr. Cook, and we have asked that you keep your comments to 10 minutes or less. Less is always preferable, but we will not hold you to anything up to 10 minutes in terms of penalties.

We may have to break from time to time for votes, which is usually about a 15-minute, although it could be longer, interruption. The faster we can go earlier on, the less likely we are to run into vote problems, so we will try to go through this.

When your testimony is over, each Member will be allowed to ask you questions of up to 5 minutes in duration. If we have time when all the Members who have come in or are available to ask questions are done, we will have another round of questions. I realize at this point, we could be going on to 12:00, 1:00, 1:30 in the afternoon. Some of you may say, I have to go or whatever. Please let our staff know and we will try to adjust the questions so that we do not mess up anyone's airline schedules or whatever it may be, but we appreciate all of you being here.

The future of money contains the potential both for great commercial promise and for enormous risk of undermining the system of exchange and the administration of justice. This is true whether

the media of exchange enter electronic commerce using computers linked into networks or via computer chips embedded in cards or other devices.

At a recent hearing on the dollar coin before the Senate Banking Committee, Philip Diehl, Director of the Mint, noted that the state of affairs with electronic forms of money was analogous to the situation before the Civil War, when local banks issued their own paper money. He foresees that, left alone and unregulated, the market may produce an electronic "Tower of Babel", with no single standard of technology and many opportunities for law avoidance and criminal transactions.

We will begin to explore these emerging third wave forms of currency and begin to define the appropriate role of the Federal Government with reference to this evolving technology. This will not be accomplished in a single day or one hearing. This morning, we will hear from a panel of six expert witnesses, all from the private sector. With their assistance, we will begin to consider some of these vital issues.

At a later hearing, governmental entities with responsibilities in the management of the integrity of our monetary system and others with responsibilities for the enforcement of laws relating to it will testify. At that time, we will consider in greater depth public policy issues raised today.

With more than $2 trillion currently moving electronically each day between U.S. institutions, the safety and security of this system is not to be taken lightly. Basic requirements are clear. Payment instruments must be widely accepted, convenient, cost effective, safe, and confidential to ensure wide usage. The legitimate law enforcement and public policy interests of the government must also be recognized. Cooperative efforts between banks as an industry and between banks and the government have made the current payment instruments successful and widely used, and if these precedents are applied in future payment mechanisms, they may be made similarly successful.

I had the occasion last night in preparing for this hearing to look at this tape on Mondex, which I am sure is familiar to all of our panelists, which Nat West has started, I guess, over in England. It all looks very easy and very simple here and everybody already seems to have their Mondex machine, which probably is not exactly the case of all the businesses in the country. But it gives you some idea of the electronic exchange of money, being able to obtain your balance and being able to travel just with a card.

We are going to have other demonstrations today. We have some stored value cards right here on the desk which we are going to see.

In also preparing for this hearing last week, I met with a constituent who has helped with this. I was told that he had purchased a flashlight via the Internet using CyberCash, which is a secured payment system. Indeed, I have that flashlight here today. This was purchased with a credit card on the computer using the Internet without any kind of other transaction and the money was transferred from one to the other. After a wait of a little while, this flashlight came.

I am not sure I would have bought this flashlight, to be totally candid with you. It has got a radio on it, it has got a flashlight, and it has got a siren, so this is a highly safe flashlight, if you will, that does a little bit of everything. But the point is not the flashlight itself. The point is that we are now able, in this day and age, even, although some of us can barely read our e-mail, there are those out there who can, indeed, make acquisitions through the Internet using CyberCash or other systems in order to do that. That shows you, I think, the beginning of the trend that we are going to see.

We are, indeed, fortunate to have before us some of the pioneers of the new electronic payments technology to discuss their creations and the implications of its implementation. By the way, I think you truly are pioneers. To save time, I am not going to go through a lot of resumes, although I am going to explain who each of you are. But I think it is worthwhile to note to the audience that we are dealing with individuals who are at the very cutting edge of this not necessarily new technology but new application of the technologies which may have existed for some time.

We are going to have each of you testify, starting with Mr. Van Lear. In order, it will be David Van Lear, who is the President of Electronic Payment Services, which I am proud to say is located in my State. Next will be Dr. David Chaum, who is the Chairman and CEO of DigiCash, Inc. Then we have William Melton, who is the Chairman and CEO of CyberCash, Inc., who brought us our flashlight here.

Then we have Rosalind Fisher, who is Executive Vice President of Visa USA, and I see some Visa cards up here. Heidi Goff is a Senior Vice President of MasterCard International. And we have Scott Cook, who has received a lot of attention lately in the news, who is the Chairman of Intuit, Inc. He is the owner and developer of Quicken, by far the leading personal finance and home banking software.

You are kind to come here today. You are kind to give us your time. We will try to give you all the time and attention we can, and you may rest assured that whatever information is brought forth here will be spread throughout the Congress so that we will all become more familiar with it.

Let me turn to the other Members and see if they wish to make opening statements and then we will turn to you.

Mr. Lucas.

Mr. LUCAS. I have no opening statement.

Chairman CASTLE. Mr. Chrysler.

Mr. CHRYSLER. I just want to welcome you here and I appreciate the card. I brought similar ones in when I testified in front of the Ways and Means Committee on medical savings accounts and gave every Member one that had their name on it. I appreciate the memento.

Chairman CASTLE. Thank you, Mr. Chrysler.

Without further ado, Mr. Van Lear, we will turn to you, sir.

STATEMENT OF DAVID VAN LEAR, PRESIDENT, ELECTRONIC PAYMENT SERVICES

Mr. VAN LEAR. Thank you. Good morning, Mr. Chairman and members of the subcommittee. It is a great honor to speak with you today at these hearings on the future of money. My name is David Van Lear. I am Chairman and Chief Executive Officer of Electronic Payment Services, Incorporated, also known as EPS.

EPS was formed a little more than 2 years ago to serve the present and lead the future development of electronic payment systems. We have become one of the leading electronic transaction processors in the United States, processing 1.5 billion transactions annually. EPS is headquartered in Wilmington, Delaware, and serves as the parent company for two subsidiaries, Money Access Service, Incorporated, and BUYPASS Corp. EPS, in turn, is owned by five major regional bank holding companies, Banc One Corp., CoreStates Financial Corp., KeyCorp, National City Corp., and PNC Corp.

Money Access Service operates the MAC shared ATM and point-of-sale network, the largest in the United States measured by transactions processed through our switch, more than 900 million annually. The MAC network is found in 34 of the 50 States. We serve 1,700 financial institutions, and these institutions operate 18,200 ATMs and 150,000 point-of-sale terminals. Thirty-two million customers carry MAC-branded ATM cards.

BUYPASS Corp., is a leader in point-of-sale processing. It serves financial institutions and merchants in all 50 States. BUYPASS's particular expertise lies in processing payments for the petroleum, convenience store, and supermarket industries. BUYPASS processes more than 500 million transactions annually.

It is from a base of over 25 years of experience in this industry that I want to speak to you today about how electronic commerce functions today and about those issues which are important to preserve public confidence in new forms of electronic money in the future.

What is electronic commerce? It is commerce which takes place using some form of electronic processing based on a means of exchange. It includes wire transfers, where an individual delivers currency to one location with an instruction to send to another, where funds are disbursed to an authenticated party.

Electronic commerce is also found in the use of credit and debit cards, which are accepted by merchants for purchases and then authorized and settled electronically. It is also the electronic processing used to dispense money or take deposits through ATMs. And, it is the electronic banking which takes place from the home telephone or computer.

In each of these examples, commerce is facilitated by money which is, at some point in time, electronic.

These electronic forms of money work because the public has confidence in the systems behind each of them. The systems have integrity. Part of this integrity comes from the involvement of financial institutions. In the United States, financial institutions have fiduciary responsibilities which assure the safety and soundness of the overall system.

Another means of assuring system integrity is through the regulation of providers within these financial systems. In the case of financial institutions, regulation comes from government. In the case of non-financial institutions which operate within these systems, oversight comes from operating regulations which contractually bind them.

Consumer confidence in electronic money is further enhanced by the system's security, which assures all participants that only the appropriate parties have access to sensitive information as well as to the funds being transferred. Privacy is directly linked to system security.

Authentication of electronic money transactions gives participants the assurance that the transactions are valid. Validity is reinforced through the ability of a central authority to track electronic transactions and post facto audit the system to maintain integrity. This tracking gives the government and system participants the ability to track the amounts of electronic money flowing through the system as well as its velocity. Both Federal and State taxing authorities can use it as a check on tax liabilities.

Jurisdiction of the system is through applicable laws. One of their roles is to protect consumers against fraud. This, then, is our current system.

As new forms of electronic money evolve, we need to ensure that participants have the same level of confidence in these new systems as they do in the present ones and we need to protect the present systems from any potential negative fallout from new, less secure services.

We believe the following issues, therefore, must be addressed as new electronic money systems are enabled. System integrity—the system must be able to be trusted to work properly every time.

Safety and soundness of system and providers—there must a high level of trust in how the system functions today as well as the fact that it will be there tomorrow.

Regulation—rules to ensure compliance to a set of standards must exist.

Security and privacy—the proper controls must be in place to ensure privacy within the system.

Authentication—a vehicle to ensure transaction validity must pervade the system.

Money supply, tracking and velocity—to the extent that this electronic money is involved in commerce, a vehicle to track its amount and velocity must be present.

Taxability—transactions cannot be so anonymous that taxing authorities lose the ability to assess sales and other legitimate taxes.

Auditability—to ensure system integrity, it must be auditable.

Fraud control—there must be measures to track, minimize, and control fraud.

And finally, sovereignty issues—there must be a clear definition as to which laws apply within an electronic money system. This involves both domestic and international transactions.

To illustrate the potential impact of some of these issues, let us turn to one of the electronic money systems which is being envisioned, transactions of business over the Internet. The Internet is

a series of computers linked together in a system where each computer is equal.

On the Internet, there is no central authority through which all information must pass. Therefore, there is no one body which can assure participants that the system has integrity. From a safety and soundness perspective, it is difficult to tell if a transaction has taken place, since there is no central authority to track and report it.

Further, there are currently no standard operating regulations for electronic money on the Internet and it is unclear as to which, if any, government or non-government regulations apply.

From a tax perspective, transactions can be conducted over the Internet anonymously. This anonymity and inability to track transactions could impact on a State or national government's ability to tax that transaction.

The Federal Reserve does not currently know how to track flows of electronic commerce on the Internet to measure both amounts and velocity of the money supply. In addition, there is no central authority to track and report on criminal activity, including counterfeiting and money laundering.

There are also implications relative to fraud and consumer liability. Who is liable in the event of lost or non-delivery of goods or defalcations on the part of third party providers? Does, in fact, the consumer bear the financial risk in a system of electronic money on the Internet?

What about the situation where a consumer buys goods from another country over the Internet but the goods never arrive because the merchant never sends them? Who protects the consumer in this instance of fraud? Do foreign laws or U.S. laws apply?

In summary, there are no laws which apply specifically to commerce on the Internet. Who will establish them? Who has jurisdiction over a transaction, the laws of the purchaser in one country or the seller in another?

The issue is not a United States only issue. It is one that impacts on every country in the world which has active computers on the Internet, presently over 10,000 computers in over 90 countries.

Today, you will hear from a number of organizations interested in facilitating new forms of electronic money. We believe that it is important to begin discussions addressing these issues.

We are not in favor of undue regulation but we do believe that proper care must be taken to ensure that participants in these new electronic forms of money are capable of having the same level of confidence in them as they do in the current systems which function well for all of us.

Let me add, Mr. Chairman, we are aware of what these issues are, and in some cases, solutions are already in place. It is our intent to assure that, at a minimum, the protections that exist in today's systems will be incorporated into these future systems. Thank you very much.

[The prepared statement of Mr. David Van Lear can be found on page 58 in the appendix.]

Chairman CASTLE. Thank you very much, Mr. Van Lear. I note that you raised a lot of questions, for all of us, as part of your testimony. We appreciate your testimony.

Dr. Chaum, we look forward to your testimony, sir.

STATEMENT OF DAVID CHAUM, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, DIGICASH, INC.

Mr. CHAUM. Mr. Chairman, members of the subcommittee, as an American who is regarded as the inventor of electronic cash, who has worked over the last dozen years or so to make the technology viable, and who is now CEO of a leading company pioneering in its commercialization, I am very pleased by the interest shown here and to be here today.

We are being forced to decide between two very different kinds of electronic payment technology. The core values we as a nation have fought for and continue to stand for are at stake. As a consequence of choosing one of the two directions, these values will be profoundly eroded. By choosing the other direction, however, they will be preserved and likely extended. Wise decisions at this critical juncture may also allow us to avoid certain other pitfalls and to realize economic leadership and growth.

I think my limited time before you is best used to briefly explain the fundamentally different approaches to security before coming to privacy, privacy technology, and its implications.

Security is simply the protection of interests. People want to protect their own money and banks their exposure. The role of government is to maintain the integrity of and confidence in the whole system. With electronic cash, just as with paper cash today, it will be the responsibility of government to protect against systemic risk. This is a serious role that cannot be left to the micro-economic interests of commercial organizations.

In order for those in government to make informed decisions, it will be necessary for them to understand the basic ways to secure transactions, particularly in different situations.

One basic form is tamper resistance, exemplified by the chip in a chip card. It is designed to be hard to modify or to read secrets from. Such tamper resistance is needed for so-called off-line payments, those in which the reader device receiving payment from a card validates payments by contacting a central system only at the end of each day. Incidentally, this and the other basic form must rely for security on cryptography, sometimes referred to as encryption, which is fundamental to all information security.

The second basic form is where the individual uses their own computer, whether a desktop, laptop, or palmtop device. Such software only is all that is needed in an on-line system, that is, a system in which the party receiving payment communicates over a network during each payment.

The trend is toward convergence of these two forms into a hybrid, since people do not want incompatible forms of money and since it offers the best of both worlds in terms of convenience. In other words, you will put a chip card into a user-friendly electronic device of your own choosing, whether on your desk, in your living room, or in your pocket, and I have brought some examples to show you. This is a CAFE wallet. I am the Chairman of the CAFE Project, which is sponsored by the European Commission. I will come back to it. You can pay either with the card or by infrared using this wallet.

The problems I see in the industry today reflect a lack of architecture, and architecture is essential when building infrastructure, which is what we are embarking on. In my view, a sound architecture must, one, include the two basic forms of security and allow for their integration into the hybrid. Two, prevent the vulnerability of systemwide secrets from being stored in every card, or nearly as bad, every off-line point of payment. And three, address privacy concerns effectively, since they cannot be addressed as add-ons or afterthoughts. Today, DigiCash systems are alone in having any of these three attributes, and their architecture has all three.

Let me turn to the issue of privacy. A recent Harris poll of the American public began by introducing respondents to all the consumer benefits of the information superhighway. Then respondents were told that in order to make such systems economically viable, payment transaction data would have to be gathered and used for purposes such as making special offers to them. But the majority of respondents still objected to any use, other than consummation of the payment, and they gave privacy as the primary reason.

Fully 82 percent of Americans today expressed concern over privacy of computerized data. That fraction has been growing steadily ever since the so-called first wave of privacy concern was triggered, when Americans began to see their name on punched cards and printed on computer-generated forms.

When people are exposed to the information superhighway, which provides an awesome glimpse of the power of modern information technology, with dropping transaction costs leading to finer granularity of payments, which we will be hearing more about later, I assume, concern will reach new levels.

Privacy technology allows people to protect their own information and other interests while, at the same time, maintains very high security for organizations. Essentially, it is the difference between, on the one hand, a centralized system with disenfranchised participants, like the electronically tagged animals in feedlots, and, on the other hand, a system where each participant is able to protect its own interest, like buyers and sellers on a town market square.

Take e-cash as an example of privacy technology. It provides a fully digital bearer instrument, a number that is itself money, just like a bank note is money. On the Internet, once someone downloads the requisite software, which takes only a few minutes, they are ready to send and receive e-cash in payments.

Security of e-cash is superior to that of paper cash, and also for the consumer, if it is stolen, it cannot be used. If someone refuses to give you a receipt, you have proof that they deposited it. If it is lost, you can get your money and records back. Counterfeiting e-cash poses the same cryptographic challenge as breaking the most sophisticated codes used to protect nuclear materials, military secrets, and other large-value wire transfers. Therefore, e-cash is certainly not a target of opportunity.

E-cash is already being experimented with on the Internet in a worldwide monopoly money trial with tens of thousands of participants. Related card technology has been licensed to Amtech, based in Dallas, for highway speed road tolls and road pricing, offering privacy instead of dossiers on everywhere people drive.

And CAFE, the related device I showed you, the European Commission-sponsored trial, of which I am the Chairman, at its headquarters building in Brussels has shown chip cards that can be inserted into electronic wallets, and so on, and provides actually an electronic ECU. Such privacy technology has even been successfully used by the participants at the most recent international meeting of data protection commissioners.

E-cash has received substantial media coverage. Consequently, the public is beginning to realize that the coming of electronic payments need not mean an obliteration of privacy. The superhighway will give consumers unprecedented mobility to choose it.

Some concern about e-cash, however, has been raised by various parties over possibilities it might open for illicit payments, but there is simply no legitimate basis for these allegations. E-cash, even when it were to achieve significant scale, is considerably less dangerous to society than automatic teller machines.

For one thing, like cash, the amount withdrawn and deposited is on record. For another, unlike cash, the amounts of money that pass through each person's hands are also on record at the bank. E-cash itself is less prone to abuse than paper bank notes because privacy is one way, which means that an extortionist, a seller on a black market, or the acceptor of a bribe is forever vulnerable to being irrefutably incriminated by the party that paid him.

Governments who stifle the new technology while it is still in its infancy, before it has had a chance to develop and to harmonize with our institutions who do not proactively support needed infrastructure, who fail to establish confidence by protecting against systemic risk, will be left behind in global competition. Countries who take clear positions based on understanding of the technology, however, and encourage needed developments stand to gain enormous growth and market leadership.

Privacy technology, whether used for electronic payments, voting, or other public expression, is the electronic equivalent of a free market and democracy. People will come to insist on it as an information human right. Thank you.

[The prepared statement of Mr. David Chaum can be found on page 133 in the appendix.]

Chairman CASTLE. Thank you very much, Dr. Chaum. We appreciate it.

Mr. Melton, we look forward to your testimony, sir.

STATEMENT OF WILLIAM N. MELTON, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, CYBERCASH, INC.

Mr. MELTON. Monetary systems are ultimately founded on trust, trust that your money will be there when you want it and its value will be relatively stable. That trust exists now in a three-dimensional world because of a strong global banking system backed by stable national governments.

We at CyberCash believe that commerce on the Internet will best be served by facilitating the transition of existing payment systems and the trust that is carried with them into cyberspace. While new payment systems and new monetary systems may ultimately evolve in the future, CyberCash believes that the best way to get

there is to build on the trust that already exists in our present monetary system.

Accordingly, CyberCash builds technology tools, tools for banks, tools for credit card associations, and tools specifically for the Internet.

If we divide the world into walk-around money that might be an electronic card and what we call net-around money that exists on the Internet, CyberCash is focused strictly on the net-around money.

Our technology tools facilitate the use of a variety of payment instruments on the Internet, but our focus is primarily on consumer payment instruments, including credit cards and checks. Of course, our technology does not actually push a credit card or anyone's checkbook over the wires of the Internet. Rather, CyberCash provides software-based technology which passes secure information over the Internet. That secure information becomes the functional equivalent of the physical plastic or of the paper check. The software-based technology tools will permit and do permit the smooth integration of the new information-based plastic cards or the new electronic checks with the older manual systems.

For example, as the credit card associations announce standards coming soon governing the use of their credit card systems on the Internet, CyberCash creates software which implements these standards. CyberCash provides this software free of charge to the banks and to the credit card associations, who, in turn, provide that software to merchants and consumers.

Software components work in unison, transporting credit card information securely to the acquiring bank of the authorized merchant. The acquiring bank, as part of their normal discount rate that they charge to a merchant, assumes then the cost of transporting that transaction through the Internet, providing CyberCash a small fee for transport. This is the functional equivalent of an 800-number call cost which the acquiring bank assumes and pays today.

Though the physical plastic may be missing from this transaction, there is much more security and much more privacy on the Internet than exists in the physical world. In this new Internet transaction, all the parties, that is, the consumer, the merchant, and the bank, are authenticated using a technology called digital signatures. These digital signatures are many times more secure than any handwritten signature that we might use today. The consumer on the Internet will no longer need to be concerned about losing his credit card. Without the consumer's digital signature, the actual card number is worthless on the Internet. The consumer can have absolute confidence that the merchant he is dealing with is an authorized merchant, guaranteed by the bank's digital signature. And, of course, the bank receives the non-deniable digital signature from both the consumer and the merchant. For privacy, all transactions are completely encrypted and absolutely protected from monitoring or tampering of any kind. Thus, on the Internet, we simultaneously achieve dramatically improved levels of both privacy and security.

Standing behind these systems is the entire strength of the banks, the credit card associations, effectively the entire American

banking system. Since the introduction of credit cards, the industry has continuously evolved systems which monitor and control risk. During this same time, they have evolved systems that provide ever more and ever more varied customer products to the consumer. Competitive pressure is the engine that drives down costs and squeezes risks out of the system.

As we move into the use of credit cards on the Internet, we urge that competitive pressures which have driven the evolution of the industry to date be trusted and be permitted to continue to drive the evolution on the Internet.

Checks and checking accounts are even more a part of our lives than our credit cards. To have a checking account, you do not have to qualify under the rigid credit requirements of the credit card industry. To receive a check, you do not have to be a qualified merchant. I often ask my friends in the credit card industry, when was the last time they used a Visa or a MasterCard to send $10 to their mother? Not recently. So checks are an important part of our economic lives.

As the Internet in many ways is making geography evaporate and the whole world exists more or less instantaneously on the PC screen on your desk, so that same technology will give a whole new utility and a whole new dynamism to that old checkbook in your pocket.

While checks are wonderful, we, as a society, are fairly well educated that checks also have some problems, generally referred to as an occasional bounce or an occasional forged signature. Well, we have some good news for you. Those same software technology tools that are being built to make credit cards safe on the Internet also make checks safe on the Internet. With the speed and the instantaneous nature of the Internet, we no longer have to worry about whether or not the check is good. We will know instantly at the time we accept it. Through the software technology tools that CyberCash is building for banks, funds will be certified prior to the check being sent. Checks received by you, received within seconds of their being sent, will be literally as good as money in the bank, because that is exactly where the money will be, in the bank.

Also, the same technology of digital signatures and encryption which we use to secure credit cards on the Internet will be used to secure checks. No longer will there be forged signatures. Digital signatures effectively eliminate forgery. No longer will there be false claims of forgery. Digital signatures are essentially nondeniable. No longer will there be theft of checks in the mail. Checks will travel over the Internet in totally secured and encrypted envelopes.

The automated check clearing system in the United States, in spite of the problems of paper transport, has developed into a surprisingly low-cost and efficient system. Most of the traditional banking system is built around the accounting for and the managing of the flow of paper checks around the country. Regulatory agencies have built systems, in turn, to ensure the safety of the banking system behind this massive flow of checks.

By enabling checks on the Internet, we are building on this same foundation. We are leveraging the experience of 100 years while simultaneously removing some of the known problems.

Perhaps most importantly, checks represent a personal relationship between the checkbook holder and his or her bank. In the new world of the Internet, that special relationship between the checkbook holder and the bank will be given a new lease on life, and this lease on life will be due to the technology of the Internet, namely instantaneous transfer of information, digital signatures, and encryption.

In conclusion, we would urge the subcommittee to join us in our optimism in seeing the enhancement of some of the old payment instruments by the new technology tools. We would further urge the subcommittee to embrace our faith in the ability of the competitive marketplace pressures to continue to bring consumers safer, more convenient, and lower-cost payment options. Thank you.

[The prepared statement of Mr. William Melton can be found on page 143 in the appendix.]

Chairman CASTLE. Thank you very much, Mr. Melton. We appreciate your testimony.

Next, we have Ms. Fisher, who is the Executive Vice President of Visa USA. I see some Visa cards up here, so maybe we will learn what they are all about.

STATEMENT OF ROSALIND L. FISHER, EXECUTIVE VICE PRESIDENT, VISA U.S.A.

Ms. FISHER. Thank you, Mr. Chairman. I speak to you on behalf of Visa and its thousands of regulated member financial institutions. Visa is an association that is owned by these institutions. Visa banks issue more than 400 million Visa cards around the world. They are accepted at more than 13 million merchant locations. Last year, Visa itself processed more than $630 billion in transactions.

While there has been much press attention recently to so-called electronic money and the role of a host of new entrants into the payment services business, I am proud to say that Visa, and most importantly, its member financial institutions, are playing and must continue to play a central role in the introduction and use of these new electronic consumer payment services. I say central role for two different but equally compelling reasons.

First, Visa and its member banks have a solid track record of developing an array of payment services that meet consumer needs, and we are confident of our ability to continue to do so.

Second, the integrity of the payment system and public confidence in it could be at risk if so-called electronic money becomes nothing more than zeroes and ones, digital signals, without the backing and central involvement of regulated financial institutions.

To the first point, the success of Visa's existing products is well known. Visa and its members offer many credit card options, such as the Visa Classic and Visa Gold for individuals and other credit card products specifically tailored for businesses.

Visa also offers the Visa Check Card, an off-line debit card, and Interlink, an on-line debit card. Debit cards, as you probably are aware, access a deposit or share draft account. Visa Travel Money is a prepaid card for obtaining local currency worldwide at favorable exchange rates, and Visa Travelers Cheques. Visa also runs the largest global ATM network under the Plus brand, as well as

an automated clearinghouse service and an electronic check imaging service.

The second reason Visa and its members must be involved in these evolving services has a public policy foundation. The integrity of the payment system and public confidence in it demands that regulated financial institutions be central players. On the other hand, we caution that premature government regulation or the failure to modify existing regulations to accommodate evolving technologies could chill or halt the delivery of new financial products to consumers.

I will comment further on this important issue in a moment, but first, let me give you a closer look at some Visa products about to be launched.

Payment cards embedded with microprocessor chips are often referred to as smart cards. Visa's first application of this chip technology is a stored value card that we call Visa Cash. This card is prepaid, with a specific amount of value loaded on to the microchip. It is an alternative to cash for consumers making small purchases, usually those under $20. We believe there is significant consumer demand for Visa Cash and it will be introduced in the Southeast later this year and showcased during the 1996 Summer Olympic Games in Atlanta.

You can imagine the convenience of driving to a Washington, DC., Metro station and not having to dig in the glove compartment for the exact change to put in the parking meter, meanwhile stopping to buy a copy of the *Post* on your way to the office. All of this can be done with the stored value card.

Remote banking is a term that is used to refer to the ability of consumers to communicate electronically with a bank in order to access a wide variety of banking services. Ultimately, it is the consumers who will decide and choose the preferred way to do business with their financial services provider.

For this reason, Visa's remote banking subsidiary, Visa Interactive, already offers or is developing interfaces to almost every access device imaginable. This will allow consumers to communicate via touch tone phone, via screen phone—and we have one over on the table to your left—via personal computer, via personal digital assistant, or via interactive television. Visa will provide a myriad of options for member financial institutions to offer their customers.

Let me turn to electronic commerce, buying goods and services over computer networks that can be open, such as the Internet, or closed, such as commercial services. In this arena, Visa's first priority is to ensure that Visa card payments made over open networks such as the Internet are secure. This means that the transmission of the card holder's payment data must be protected from snooping by others on the network, that the merchant and the consumer are assured that each is a valid, permitted user of the Visa system, and that, in the end, the merchant will be properly paid and the consumer billed.

Accordingly, Visa has worked with Microsoft to build a standard for secured transactions in an open network. This will give consumers and merchants the confidence and protection they need to use this new purchasing medium.

Public confidence in Visa's member financial institutions and the payment services they provide is high, and there is good reason why this is so. They are regulated by the Federal banking agencies and are subject to regular examination by those agencies and State supervisors. Customers' funds are protected by the safety net of Federal deposit insurance. A high degree of public confidence in our members, as well as in their products and services, is essential for economic stability and growth.

Some electronic payment services may be offered through entities that are not subject to the same supervision and regulation as Visa's members. To the extent that these entities enjoy an unfair competitive advantage, they may worsen the disintermediation of traditional depositories.

For these and other reasons, the subcommittee should know that a recent report by the European Union Payment Systems Working Group proposed that only banks be allowed to issue stored value cards. Visa agrees that only depository institutions or their affiliates should be permitted to issue open system stored value cards, in contrast to single use or closed system cards, such as those used in the Washington Metro.

Policy makers must be alert to the potential economic consequences from a loss of public confidence in cards issued by unregulated, uninsured companies. Law enforcement officials combating criminal activity such as tax evasion, counterfeiting, and money laundering should consider the consequences of stored value card systems that, unlike Visa's, may not generate a well-defined audit trail or whose record keeping is not subject to regulatory examination.

At the same time, government must guard against regulation that would stifle innovation. The potential application of the Electronic Funds Transfer Act and Regulation E to stored value cards is an excellent example. Regulation E requires that consumers get paper receipts for electronic funds transfers, such as ATM transactions. If applied to stored value cards, the product will fail.

Some of the most practical applications of the card will be at vending machines, parking meters, and other locales geared to small dollar transactions. Stored value cards simply will not be economically feasible if vending machines and parking meters must be reengineered to provide a paper receipt for a 75-cent Coke or 30 minutes of parking time.

Also, keep in mind that one need not have a banking relationship to get a stored value card, that the card issuer may not know the buyer's name and address, and that the value on the card may be used quickly. In this setting, the periodic statement requirements of Regulation E are totally impractical. These cards will be sold at a variety of locations, including dispensing machines, such as those used to dispense Metro farecards for the DC. transit system, and it is not economically feasible to equip these machines to collect, store, and transmit all the personal information needed to comply with the periodic statement requirements of Regulation E.

These are only a few examples of how product development, if shaped by regulation rather than by market forces, would be stunted. Other countries have encouraged innovation by letting products take shape without undue governmental interference. In order to

encourage development and to create an environment in which the United States can assume a leadership role in these endeavors, we need to do the same. We urge Congress to avoid adding to the regulatory burden of depository institutions and permit the public to enjoy the benefits of new products and services that Visa and its members are bringing to market.

One final thing. You have on the table in front of you two cards. One of them is a stored value card, and you are welcome to, after the hearing is over, to come down and use it on the vending machine. David will show you how it works. Basically, there is $20 of value stored on your card. When he puts it in there, it tells him how much he has left. Select the items, and you can have your favorite snack.

Chairman CASTLE. Do we get to keep those items? [Laughter.]

Ms. FISHER. The other card is a prototype of a chip card that actually has writable storage on it. It is a more advanced version of the chip card that we anticipate coming out in the near future.

Once again, thank you for the opportunity to testify.

[The prepared statement of Ms. Rosalind Fisher can be found on page 146 in the appendix.]

Chairman CASTLE. Mr. Flake has asked me if that is above the gift limit, whatever is on that card. You have to worry about these things in Congress. [Laughter.]

We appreciate your testimony, Ms. Fisher, and look forward to demonstrations at a later time. I have had problems with that type of machine not quite dispensing an item. Will you be able to help with that problem? [Laughter.]

Next we have Heidi Goff, who is a Senior Vice President of MasterCard International. Heaven forbid we would ever have Visa without MasterCard here, so we have you next to each other. [Laughter.]

Ms. Goff, we look forward to your testimony.

STATEMENT OF HEIDI GOFF, SENIOR VICE PRESIDENT, MASTERCARD INTERNATIONAL, INC.

Ms. GOFF. Mr. Chairman, members of the subcommittee, my name is Heidi Goff and I thank you for the opportunity to testify today. I am the Senior Vice President for Global Point of Interaction for MasterCard. You probably have never met someone whose title is "Global Point of Interaction" before. It is a new title to me as well, and it makes sense only in the brave new world described by my colleagues on this distinguished panel.

Until very recently, we expected financial transactions to take place at a certain point of sale, usually in a store, and increasingly over the telephone. The point or place of business was usually dictated by the merchant or service provider. However, in the point-of-interaction world, the sale takes place wherever the consumer wants it to—over the phone, via the Internet, from an interactive television, at a kiosk located in an airport, even the old fashioned way, at a department store.

My job is to help this point of interaction to be wherever and whenever convenient for the consumer, providing consumers with a degree of control and financial empowerment never before experienced anywhere in the world. We are undergoing an unprecedented

convergence of exciting technologies, which, until recently, resided only in the realm of science fiction.

What I want to do this morning is to leave you with a flavor for the scope of change we are anticipating, the potential benefits for consumers, and the importance for government policies which nurture the development of new era products that empower consumers.

The forces for change include technology advances in communications, integrated circuits, image processing, data storage, and artificial intelligence. Telecommunications are faster and more ubiquitous. Integrated circuits are finding their way onto transaction cards throughout the world, vastly increasing the ability to provide payment services in a secure manner.

In addition to the storefront on main street, merchants have migrated from catalog and telephone sales to electronic storefronts on information networks, such as America On-Line and Compuserve, and they are on the Internet. Consumers now browse through product images at their convenience, in their homes, making purchasing decisions with maximum information and no pressure.

Changing consumer behavior is having a profound effect on how transactions are made. Consumer research tells us that time is one of our most highly valued commodities. For the payments business, that means giving consumers the services and access they want wherever and whenever they want it.

At the same time, people are becoming increasingly comfortable with technology. Almost half of the U.S. households have computers, and as prices come down, those numbers will go up. Just look at the increase in the use of remote delivery methods, such as ATMs and cash dispensers. A recent study found that 77 percent of all U.S. households use remote delivery for at least part of their banking. The younger the consumer, the greater the tendency not to go to a teller. Right now, technology-driven transactions account for more than half of all banking transactions.

As I mentioned, new technology is now enabling new payment methodologies, such as stored value or prepaid cards, as well as new security measures which will protect consumers from more sophisticated criminals. Smart cards will improve the way we make payments and create new value for the consumer and the banking community.

Since a smart card has greater storage capacity than today's magnetic stripe technology, the card can support multiple functionalities. In other words, it can be a credit card, a debit card, and a stored value card wrapped into one. It can also store other information, such as frequent flyer or loyalty program points or discount coupons. The consumer will decide what information is stored on the card, what functionalities it will contain.

Stored value cards will allow merchants to accept card payments without the expense of maintaining on-line connections to issuers. Once the card is validated, the cash value is deducted from the card and the consumer can load more cash onto their cards as needed from an ATM, and ultimately from a telephone, almost anywhere they happen to be. The loyalty programs and coupons maintained on chip cards have endless possibilities for merchants to

give discounted goods and services instantly at the time of each transaction.

The smart card can also offer consumers greater security. By encoding the card with a personal identification number, a merchant terminal can verify the card holder without ever going on-line. The card holder simply inputs his or her PIN, the card and terminal interact to authenticate the PIN using secure cryptology, and if the PIN is correct, the card is accepted. Through unique card authentication methodology, the terminal also will validate that the card is authentic, not counterfeit.

MasterCard, Visa, and Europay have been working together to develop a single global standard for smart cards and the terminals that accept them. We want to be sure that, just like today's credit cards, any terminal will be able to accept any card. Our progress has been impressive. Already, specifications for cards and terminals have been developed.

While chip technology will add greater flexibility to payment cards, increased connectivity is giving consumers broader acceptance for those cards. As a result, the point of sale, a physical place defined by the merchant's location, is migrating to a point of interaction, a virtual place defined by the consumer's location.

There are two pieces to the connectivity equation, expanded networks and a growing number of on-line services. By networks, I am talking about the physical connections rather than services. Three of the most commonly recognized are telephone networks, cable networks, and satellite services. Each of these networks offers a potential path for carrying value transactions. Consumers can do their banking by phone. In some places, they can bank on their television screens.

The bottom line is that the availability of these expanded networks increases our ability to serve more consumers efficiently and effectively.

On-line services are the other half of the equation. While there are more ways to hook in, there are more things to hook to. The electronic superhighway is expanding exponentially. Every day, new services become available and every day the traffic becomes heavier. More than 25,000 merchants in 150 countries are already on the Internet and it serves 20 million users right now. By the year 2,000, we expect it to be more than 100 million. It is safe to predict that, in the future, anyone who has anything to sell will be connected to it, as well.

One important role for the payments industry will be ensuring that those value transactions are secure. Right now, with few exceptions, if you send your account information across the Internet, you may be leaving yourself vulnerable because those transactions are conducted on unsecured lines. MasterCard, together with Visa, has been working to ensure that on-line transactions can be made securely, and by year end, that will be a reality.

We are also acutely aware that many consumers feel that the greater access to information raises concerns about consumer privacy. Last year, we joined with Yankelovich Partners to assess the privacy concerns of today's consumers. We also looked at the potential for using personal data for better fraud protection and improved consumer satisfaction. We recognize that if consumers do

not trust us to protect their privacy, they are not going to use our product. The bottom line is, consumer trust is key to our continued success.

Finally, we appreciate that Congress has an equally significant role to play in ensuring that the consumer receives the value we are promising, the broadest range of products and services, unsurpassed acceptance at all points of interaction, and top-quality customer service and security, no matter where the card holder is. As new financial services and products are developed, we look forward to continuing to work with legislators and regulators who have oversight responsibilities.

Without question, though, we will be consistent in our message to you. That is, nothing would do more to prevent our ability to make good on this commitment than premature regulations. We urge this subcommittee to continue its efforts to study the products and services we are discussing and to play a leadership role in guiding Congress to be a partner in development.

Thank you again for the opportunity to introduce you to our view on points of interaction. We look forward to working with you to create a future that serves the best interests of both consumers and American financial institutions.

[The prepared statement of Ms. Heidi Goff can be found on page 163 in the appendix.]

Chairman CASTLE. Thank you very much, Ms. Goff. We appreciate your fine testimony.

Our clean-up hitter, at this hearing, at least, is Mr. Scott Cook, who is the Chairman of Intuit, Inc., and as I have already indicated, the owner and developer of Quicken, which is, of course, a business system that many, many people use already. Mr. Cook, we look forward to your testimony.

STATEMENT OF SCOTT COOK, CHAIRMAN, INTUIT, INC.

Mr. COOK. Thank you. Mr. Chairman and members of the subcommittee, I want to thank you for the opportunity to speak this morning. Let me begin with an orientation to electronic commerce.

Intuit is involved in an entirely different part of electronic commerce than some of today's panelists. For example, some companies are focused on creating new payment systems. Some companies are focused on allowing people to purchase goods electronically. Intuit's focus is different. Our focus is on providing people and small businesses with PC technologies to help them make better financial decisions. We are not creating new kinds of money.

If you know my company at all, you probably know us for our first and flagship product, which has been mentioned, Quicken, which is the world's most widely used personal finance software. In fact, it is the Nation's best-selling software application program.

However, Quicken is just one of our products that we make to achieve our goal of improving the financial lives of consumers and small businesses by helping them make better financial decisions. The others include the Quicken Financial Planner, which is the Nation's best-selling financial planning software; TurboTax and MacIntax, which are the Nation's best-selling software products that help you file your income taxes; the Parents Guide to Money, which is software that helps parents with the four important finan-

cial decisions they make, on life insurance, health insurance, child care, and college savings; and the Quicken Mutual Fund Selector, which gives consumers unbiased information to decide which of thousands of mutual funds meet their objectives.

Also, for small businesses, we make QuickBooks, the Nation's leading-selling accounting software, and QuickPay, the Nation's leading-selling payroll software.

We also proudly export American technology. To date, our products are the best sellers in every country that we have entered.

Let me demonstrate what I mean by enabling people to make simply smarter financial decisions. Let us look at one example, retirement planning. We all know that structural changes in pension and Social Security benefits have moved the burden of funding one's retirement onto the consumer's shoulders. Yet, when I speak publicly, I ask audiences sometimes whether they have in place a retirement plan that they know will take care of them when they retire. Stunningly, only 5 percent of the audiences I speak to raise their hands, and that is a national tragedy in the making.

Millions of working Americans will retire in poverty, not in prosperity, unless they put a retirement plan in place in the next few years, yet only 5 percent have done so. Why do they not? Because financial planning is just too complex for consumers to do unaided, and truly unbiased financial advisers are so expensive that only the very rich can afford them.

We at Intuit are trying to change this with software we just introduced this spring, called the Quicken Financial Planner. It delivers an unbiased retirement plan, personalized to each consumer's specific situation. What I would like to do is demonstrate briefly how that operates.

What we found out was people just do not know how to begin, nor do they know the steps to go through to do a retirement plan, so we have built this in a step-by-step fashion. In fact, that is the headline here, confident retirement planning step by step. All the user need do is hit the next button down here and answer the questions that appear. This first screen describes the process. This next screen details the specific steps the customer will go through. I will hit the next button to continue.

The first step is entering personal information. I will hit the next button again, and up pop the first questions, the customer's name, birth date, and desired retirement age. Hit the next button again and questions come up on health and other matters to help begin estimating life expectancy. So in this process, the customer goes through the product.

Whereas these questions are fairly easy, some questions are more challenging. I am going to jump ahead here to the taxes and inflation section. Here we need a place for the customer to enter what the rate of inflation is, in case it should change. However, if you ask anyone to estimate the rate of inflation for the next 50 years, they are not going to be able to answer that question, so what we do is work with noted financial experts, in this case, Jane Bryant Quinn, who actually suggests 4 percent as currently the best rate to use.

But then if a customer ever has a question, the user can just click the "expert" button, as I just did, and what pops up is not dry

text on financial matters but, in fact, what pops up is Jane Bryant Quinn herself.

[Audio of Ms. Quinn was played.]

Unlike real experts, you can turn them off. [Laughter.]

In this way, the customer can go through answering questions about their assets, their loans, their income, expenses, their retirement benefits. I will jump ahead to results, where the customer can see their financial picture from now through their expected death, in this case, their income. You can click on expenses here and see expenses. This bulge here is the college expenses of their children.

You can go out and click on portfolio, and here we can see one's investable assets. Here, you can see in this customer's case, there is a problem. The money runs out before they do. That is why up top here we say, your plan fails, but you have assets you can sell. Namely, you have a house you can sell.

But we do not leave the customer hanging there. Instead, I will hit the next button a couple times and get to a "what if" area, where this shows that I have 79 percent of my retirement funded and I can now play with the fundamental assumptions to see what it will take to sufficiently fund my entire retirement. So I can try to save some more and then recalculate and see, no, that does not do it. Let me save a little bit more. No, that does not do it. Maybe I should retire a little bit later. Let us go up here to maybe 63, and now recalculate, and boom, now I have a plan which will sufficiently fund my retirement.

This is the kind of work that we believe will make dramatic improvements in people's preparedness for retirement. This product costs $39, which makes financial planning available beyond just the richest 3 percent of households, and, in fact, puts it within easy reach of the 30 percent of American households who now have PCs. That is a tenfold expansion in availability.

Mr. Chairman, just a few days ago, my company announced another move that we are making to enhance people's ability to make better financial decisions, and this is by giving them a communication link to their bank that will facilitate the delivery of rich financial information in an automatic fashion.

We are working with 17 of America's largest and most trusted banks, plus American Express and Smith Barney, to connect them electronically to Quicken users. This work is based on a simple premise, that customers and financial institutions both seek closer and deeper relationships with each other. I have not met a banker yet who did not want closer relationships with their customers. Similarly, customers want to be able to deal with their bank whenever the customer wants, including weekends and nights.

What we are building is a method of communication that will enable that to happen, that will enable banks to be able to reach and serve their customers in the convenience of the customer's home or offices whenever the customer wants, 24 hours a day, 7 days a week.

The financial institutions benefit by cementing relationships with their current customers, as well as finding ways to gain new ones. Longer term, there will be some nice cost implications. Ultimately, the cost of electronic commerce is built upon the fundamental cost

of silicon and of software, two cost elements which go down and have been going down for years.

Such a trend can only help banks become more competitive in a financial services market that is truly global, and this is good news for the American economy and for your constituents, whose taxes guarantee bank deposits.

Keep in mind that electronic commerce has many suppliers. Electronic commerce will be a lot like magazines or radio stations, where there are dozens or hundreds of competing interests.

One last point about electronic commerce is that there are other benefits here, as well. With software like ours, people will be able to achieve their financial goals better than they have in the past. Thus, people will avoid some of the problems that sometimes they run into in their finances. There will be fewer bad debts, fewer personal bankruptcies, and a higher savings rate here in the United States. This is our mission and what we and our financial institution partners are committed to.

Finally, Mr. Chairman, I have not come here today to seek any action. I am here to provide you with information. However, to the extent you move forward in this area, I would ask you to consider that there are many excellent rules already in place to protect consumers and ensure a strong banking industry. Many of those rules were written before PCs and some of them might need to be updated to reflect what PC-owning consumers want.

Thank you, Mr. Chairman, and with that, I will be glad to respond to any questions that you or other Members of the subcommittee may have.

[The prepared statement of Mr. Scott Cook can be found on page 168 in the appendix.]

Chairman CASTLE. Thank you very much, Mr. Cook. That was an interesting demonstration of electronic commerce.

A lot of this is new to me, and I am probably fairly safe in saying new to many members of the subcommittee, if not all members of the subcommittee. We appreciate all of you coming forward. We do think that this is an important area for us to examine.

Let me just briefly, before I go to the questioning, just say that we, as I indicated in my opening, will be having another hearing, probably in September, at which we are going to have our government officials here to tell us about their concerns. Actually, a lot of you did speak about security—I may ask a question about that—which I thought was interesting, because we do have that concern. As Mr. Cook has said, many of these rules are probably valid but maybe need to be updated because of the use of PCs and electronic commerce and areas that we have not used heretofore.

For the format of the questioning, for the members of the subcommittee, as I have already mentioned to the witnesses, we will have our usual 5-minute rule of questioning. I realize when you have six people, one question can be destructive of a Member's time, so I have asked the witnesses if they could hopefully have not more than two answer any particular question so you can ask other questions. If the members of the subcommittee wish to cut it off and get to another question, please politely try to do so, and I hope the witnesses will understand we have a limited time.

If we get through a round of questions and there is still interest and time and you can still be here, perhaps we will have time to go through a second round, but I want to make sure everybody has an opportunity.

I just wrote some notes down as we went along and I will just start. These are general questions as opposed to specifics of any of you, but I just wanted to put some of these forward.

My first question is, will the things that we have talked about here today, electronic commerce in general, stored value cards, using the Internet to do transactions, complement or replace the existing banking and purchasing systems we have over some period of time? It seems to me that the timeframe for these kinds of things is never very predictable. It is sort of like the inflation rate that was mentioned earlier. It is very hard to say if, in 5 years, we will all be using our computers to do this or it is going to be 10, 15, or 20 years, so I am interested in that length of time that may go into it.

Just how soon the future is going to arrive, I guess is the question which I have. I know that is a very broad question. I know it is not quite predictable, but if any of you want to take a stab at it, I would be interested in hearing your views on the timeliness of all of this.

I did not think you would be this shy, not this group.

Ms. FISHER. I will take a shot at it. Mr. Chairman, I think, first of all, to your question about whether it is complementary or replacement in terms of the new technologies, clearly, we are in a complementary phase now where we are evolving to the new world as we maintain and continue to have products and services that are based on the foundations that we have put together.

In Visa, working with our member banks, we have in place a very fine payment system that, in fact, is accountable and has systems in place that do the kinds of work we need to do to consummate payments.

In terms of how soon will the future arrive, to a large extent, the marketplace will dictate that, and that depends on how consumers react to the products, and frankly, this group, Congress, has something to say about that in terms of how much we regulate or do not regulate. But I think if the market is allowed to evolve and consumers can choose to accept the products as they arrive, then we will see it move more quickly.

Chairman CASTLE. Thank you.

Heidi Goff mentioned that half the households, I believe, have computers, and 77 percent, did you say, use electronic banking?

Ms. GOFF. Seventy-seven percent of the households use electronic means of banking, such as ATMs and remote delivery. That is from a BAI study from 1994.

Chairman CASTLE. Right.

Ms. GOFF. Then I also mentioned that almost half of the households, although Scott said 30 percent have—I am sure we each have a way of counting. We do have some research that would suggest that it is coming close to 50 percent and that people will continue to use the methodologies to conduct their finances. We expect it to be—I would agree with everything Roz said. We would expect

these payments to be evolutionary and to be part of the infrastructure that the banking system has already created.

Chairman CASTLE. Let me ask you maybe a follow-up to that. What about that portion of our population which either cannot afford to plug into these systems, if a computer is going to be an element of it, or because of other limitations or just, perhaps, blocks of their own, such as perhaps I have in using computers, whatever it may be, either cannot afford or choose not to use these services. I assume we are not devising a system that would completely abandon the kind of hand system that we have today, inefficient as it may be.

Ms. GOFF. Absolutely not. I think that, just like credit cards 25 years ago were for the privileged few, today credit cards are rather an expected convenience in the American society. Debit cards, ATM cards now provide electronic access to deposited funds. And stored value cards are really a form of cash. They will not be restricted to people who have depository accounts or who have credit card accounts. They are really products that can be used by anybody in the society.

Chairman CASTLE. Let me ask one more question. What is the cost of a simple transaction, like the acquisition of this incredible flashlight which I demonstrated earlier, as compared to, for instance, having called them and given them either your Visa or MasterCard number and gotten it through the mail that way? Are the costs roughly the same, and who bears these costs, or is it more expensive?

Mr. MELTON. Obviously, the answer is different, depending on several situations. But in that specific situation, which I do know something about, the cost when the systems all get into place will be dramatically cheaper doing it that way. A lot of the risk goes out of the system. If you were to call today over the telephone and give your information in the open, the merchant would have a higher discount rate than if you were in front of him face to face. With the new systems that Visa and MasterCard are now designing and putting into place, a lot of the risk goes out and they will be able to make the cost over the Internet as cheap or cheaper than a face-to-face transaction.

Chairman CASTLE. Let me ask one final question, and that is this whole issue of fraud and security. All of you were very careful, or practically all of you, were very careful to mention the various safety nets that are built into it and, indeed, talked about dealing with banking institutions and electronic commerce and expressions such as that, which is all well and good.

But we all know that every time some system is created that involves money, there are pirates out there immediately trying to devise some way of getting around it. It seems to me that we have read about the great computer glitches in the past, which is a whole other issue that we have to worry about. I worry about the pirates. I worry about fraud.

I trust, if it was up to all of the operations of the various entities you represent, this probably would not be a problem because you have been in existence for some time. You are the pioneers; you have developed these things. But I am worried about the next

group who is sitting at home, who is a hacker someplace trying to figure out some way to rip off these systems.

This is obviously the subject of a later hearing which we are going to have, but I would be interested in your views on this, not from your own systems but from what we are going to have to do to monitor the changes to the use of electronic currency and what the government should be doing with respect to making absolutely sure that we are not going to have dramatic runs that could not be expected in banking today or other priority transactions which would be a problem, if any of you have given any thought to that.

Mr. CHAUM. I think it is a new medium. Just like the answer to your first question, probably there will be an enormous explosion in commerce on the information superhighway because it makes a tremendous lot more goods and services available to people much more easily. It will create whole new markets. It is not really a matter of evolution.

Similarly, since it is a new medium, there will also be new vulnerabilities, but on the other side, there will be much better protection than we are accustomed to in many cases. So it is different. That is my personal view.

Chairman CASTLE. Thank you.

Let us, if we can, turn to Mr. Flake, who is the ranking minority Member on the subcommittee. He has been a wonderful gentleman to work with and, I am sure, has questions for you.

Mr. FLAKE. Thank you very much, Mr. Chairman.

I do have an opening statement which I would like to submit for the record.

[The prepared statement of Hon. Floyd H. Flake can be found on page 48 in the appendix.]

I only regret that, since I did not have breakfast, you did not take a break between the testimony and questions so that we could go over and have our snack. [Laughter.]

Nevertheless, the question that I have has to do with the fact, Mr. Chairman, that we have had hearings here regarding whether or not we ought to convert the paper dollar to coins. Here we are today with the subcommittee that is far beyond, it would appear to me, any discussion about paper or coins.

I just wonder if the subcommittee might have a reaction, given that it seems as if by the time we make the decision which direction to go with this, coins or paper will be so archaic and out of use that we will have expended millions and millions of dollars to create coins, if we use coins in place of the dollar bill, that will not have any uses. You cannot use them in the laundromat. You cannot use them to buy snacks.

Can I get an opinion from someone in terms of that? I know this is not the hearing for that, but I think it is important to have on the record some sense from persons who are involved in what I consider to be the next phase of the evolution to whatever kind of monetary practices we are going to have operative in the future.

Mr. CHAUM. I would like to say one thing, just based on the European perspective, very briefly. I have been involved with the European Commission study of how to replace national currencies by an ECU, and we have done a lot of consumer surveys. People are very happy to have an electronic ECU and it is an enormously cost-

ly process, as you can imagine, to switch physical currencies and to manufacture them. It is also very time consuming. So an electronic ECU has a lot of appeal. It probably can be more secure, more cost effective, and still retain the same privacy that people are accustomed to with cash.

Mr. FLAKE. So in your opinion, or in anyone's opinion, does it make sense for us to even give major consideration to the thought of changing the paper dollar to coins, or is that an archaic discussion already?

Mr. COOK. Mr. Flake, I cannot speak to the merits of the issue of coin versus paper but I can say that my expectation is that physical currency will be with us for the rest of our lives.

Mr. FLAKE. OK.

Mr. COOK. Certainly e-mail, for example, is a wonderful invention, but the U.S. Mail is still here and is as popular as ever. Certainly new forms of transportation have been invented, but old forms still exist.

The consumer habits change very slowly. Do not get caught up in the PR hype in the press. This stuff is interesting. It will be popular, but it will not replace the existing means that are known and trusted, and in my view, it will not replace them in our lifetimes.

Mr. FLAKE. Thank you.

Mr. COOK. It is a nice complement. It is not a replacement.

Mr. FLAKE. It will not replace it.

Mr. VAN LEAR. Mr. Flake?

Mr. FLAKE. Yes.

Mr. VAN LEAR. I would like to just add that we have been talking about a paperless society for the last 25 years and checks have been predicted to be out of our society 10 years ago. They are currently still growing, at a relatively slow rate, but they will continue to be with us for that period of time, as well.

So I think the ability to move consumer behavior, particularly as it relates to payment system mechanisms, is a very slow process. ATMs took 25 years to mature in this environment to the point that people are comfortable using them now, not only to take money out but to put money in.

Mr. FLAKE. Thank you.

Presently with cash, once a transaction is completed, it is virtually impossible to trace who made the purchase. Many Americans value this anonymity when conducting their business. This technology has the possibility of tracking people and keeping complete records of their purchases. This is a plus when it comes to servicing an underground criminal economy but can definitely encroach on the privacy of law-abiding citizens.

My question is, will stored value cards keep financial transactions anonymous or is this an area of concern that we in the Congress ought to be addressing?

Mr. CHAUM. I would like to respond to that briefly. This is a card which does provide perfect anonymity for low-value payments. There are also many who offer what I call pseudo-solutions to this problem, and they suggest that if one is able to buy a card without having to identify one's self, then this provides a kind of privacy. This is a false and bogus argument simply because the card identi-

fies itself in every transaction and all those transactions can be linked and collected together.

So when you use a French phone card, your name is not on it, you did not identify yourself when you bought it, but someone can go through the data base of all the phone calls that are made and find all the calls that were made with that card, perhaps trace that to your home phone or your office, and in that way associate a particular card with you. Then it is even worse than if your name were written plainly on the card, because people have the false sense of security that their anonymity or their privacy is protected whereas, in fact, it is not at all.

Mr. FLAKE. I would just ask the Chairman for unanimous consent for 30 seconds. Can you define for me perfect anonymity? How do you determine that a card has perfect anonymity versus another card that would not have that definition?

Mr. CHAUM. This is the subject of the *Scientific American* article, which I think I have made available to all of you. The essential idea is that some cards reveal identifying information as an intrinsic part of their security mechanism. In fact, most of the techniques which you have heard about here from my colleagues are of that type.

There is another type, a second type, which is fundamentally different, which simply does not reveal identifying information in the process of making a transaction. That is what I have called privacy technology in my presentation. We have developed it for the European Commission. We developed it for automatic road tolls, for e-cash on the Internet, and so forth. It is a very versatile and very competitive technology.

It just depends on what you want to do. Do you want to build a system that basically undoes the kind of freedoms that are the basis for our society? There have been a number of think tank reports that come out of Washington that suggest that the best way to turn this into a police state would be to use identification-based payment and outlaw currency, bank notes, and coins. There are studies to that effect.

Do you want to do that, or do you want to allow the electronic medium to give us preservation of the level of privacy that people expect to have today? What we have shown is that technologically, that is certainly feasible. It does not cost more and it can be done. But left to their own devices, at the moment, the financial services industry has not really adopted this approach and what they are building is something that will give them more and more detailed information about people's activities. I think those are the two different approaches that I alluded to in my presentation, that I said were really fundamental to the things that this country stands for.

[The *Scientific American* article referred to by Mr. David Chaum can be found on page 137 in the appendix.]

Mr. FLAKE. My time is expired. Thank you, Mr. Chairman.

Chairman CASTLE. Thank you, Mr. Flake.

Mr. Royce.

Mr. ROYCE. Thank you, Mr. Chairman.

I have an opening statement which I would like to insert into the record.

[The prepared statement of Hon. Edward Royce can be found on page 52 in the appendix.]

Mr. ROYCE. I guess there are two slightly contradictory observations that you have made here today. One is that e-cash or digital money would best be shaped by market forces rather than regulation, that we should have as little regulatory burden as possible, and Ms. Fisher suggested two areas where we could pull back that burden.

At the same time, each of you have said that we need safety and soundness and a high degree of trust, and therefore a high degree of government control over this emerging process, with the exception of Ms. Fisher, who has suggested that we could use backing of regulated financial institutions in place of that evolution. Mr. Van Lear, I think, said that the role of government is to protect against systemic risk, or that was Dr. Chaum.

So the basic assessment here is that it is government control of the emerging system that you are going to rely upon for that measure of safety and soundness. What I would argue, for you to think about, is that in the Western world, governments routinely debase their currency. Governments do a very bad job of managing the value of the currency.

If you look at the boom-bust economic cycle and the millions wiped out every time we go down on the down-side of liquidation, if you look at the problems with inflation and the fact that a nickel today is worth a fraction of what it was a couple generations ago, and if we look to the future with a $5 trillion debt here in this country, to give just one example, and try to imagine what is going to happen if that debt is monetized in the future.

In terms of the problems with counterfeiting that has been pointed out today, if you look at the counterfeiting problems that we have with the U.S. dollar right now in Eastern Europe in the Independent States, that is a problem of incredible magnitude right now in terms of counterfeiting of $100 U.S. bills.

So all of these problems already exist, and I guess I was looking at it from the opposite perspective. I was in the hope that the evolution of digital money might bring pressure to bear on the existing monetary system to encourage an end to this debasement of the currency and that somehow the evolution of a new system would encourage and leverage for a stable unit of exchange.

If any of you would like to make comment on, 20 years down the road, a generation from now, where might we be, could this leverage for such a stable monetary unit in international exchange?

Mr. COOK. Mr. Royce, let me just address the opening of your question about the panelists seeming to be in agreement requesting more regulation in this nascent area. I did not talk much about regulation, so let me make my point of view clear. I do not believe this is a place that will be aided by a host of new regulations or legislation. It is so nascent, so at the beginning, it is so hard to determine what consumers really want and in which direction it is going to go.

I think regulation would likely stunt developments here, not help developments, and so I do not believe that this is a fertile field for new regulation. As I mentioned, there may be only some tuning of existing sound regulation that was put in place before computers

were envisioned, which is a very different matter than additional levels of regulation. And, in fact, I believe those sorts of changes can largely be achieved working directly with the regulatory agencies without a need for legislative involvement, and if there is a need for that, we can get back to you.

Ms. GOFF. We would like to add to that that we would very much like to work with the legislature and the regulators to monitor and develop new products but that it is premature for any regulation at this time on evolving products and services.

Mr. ROYCE. Now let me ask Ms. Fisher, if I could, it seems as though the Federal Reserve Board will have a diminishing role in the payment system. Do you currently compete for business with the Fed, for instance, with your automatic clearinghouse? And with the advent of forthcoming technologies, what will be the Fed's role in the future?

Ms. FISHER. We do with our automated clearinghouse service provide a private sector alternative to the Fed for ACH processing, which I believe was a requirement, that the Fed needed to open it up to private sector providers, and Visa did step into that breech. I believe there are a couple of others who also provide private sector alternatives. So in that sense, yes, I guess we do compete, but that is something that I believe Congress required, that the Fed offer it.

Mr. ROYCE. What market share would you say you have now?

Ms. FISHER. I do not have the exact figures. I can get that to you, but my guess is that it is something less than 25 percent.

Mr. ROYCE. Thank you.

Thank you, Mr. Chairman.

Chairman CASTLE. Thank you very much, Mr. Royce.

Mr. Metcalf.

Mr. METCALF. Thank you. I also have an opening statement which I would like to insert into the record.

[The prepared statement of Hon. Jack Metcalf can be found on page 54 in the appendix.]

This is a fascinating discussion. I am going to follow up a little bit on Congressman Flake's excellent question.

We are all talking about how money moves or works in society. I believe we are missing a major and fundamental point if we do not carefully consider, how does money arise? How does it come into being? Where does it come from? The Fed is concerned about money supply. How does e-mail fit into money supply? The founders are deeply concerned about who has the authority to create and issue money. Jefferson and Madison, two of our most insightful Presidents, were very concerned about this and they said, only government should issue money.

Is there any finite control? Who is responsible? Do you create money?

Ms. FISHER. Let me say that the Visa approach here does not create electronic money. The idea here is that we are trying to facilitate the use of the existing Visa products and services on mechanisms such as the Internet and other networks.

So we are not talking about the approach taken by some others in the industry who are creating a new form of cash, if you will. Rather, we are talking about using existing products that financial

institutions offer today but providing a safe and secure way for those existing products to be used on new technologies, new networks, in the new environment.

Mr. METCALF. Do you not monetize credit, and is that not a money creation? I think you do. I think you do, but I may be wrong. You go ahead.

Ms. FISHER. The Visa cards offer a form of payment, yes.

Mr. METCALF. A form of payment?

Ms. FISHER. Is that what you were referring to, creating cash or creating——

Mr. METCALF. Yes. Do you not monetize credit, in a sense, when you issue a credit card and allow people to create money? Is that not a money creation?

Ms. FISHER. I do not think so, sir.

Mr. METCALF. Does anybody else want to try on that one? I think this is a fundamental question. We have pretty strict—the power to create money is an incredibly important power. If people are creating money, and you were all talking about how money moves but nobody is bringing up that. I guess I think that is a fundamental question, and I think our society is at fault in not looking at that question. Where does money come from?

Mr. MELTON. I will take a swipe at a very narrow answer to that. At least for our services and the technology tools that we provide, in our world, we are only providing transport, but in all cases, we are going back to working with the banking system.

The banking system, as a whole, certainly does create money. The banking system is highly regulated and with their minimum requirements, then, in terms of equity base, they do make loans and that whole process of making loans does create money, but it is the regulated process blessed by the government.

Now, all that we are doing, and, in fact, if I may speak for the credit card associations, all of their credit that is issued through the cards comes out of a regulated bank and that bank is doing through the plastic what it could just as well be doing over the teller's counter or over the loan window.

Mr. METCALF. So banks can create money, too?

Mr. MELTON. Banks as part of the government franchise given to the banks, yes.

Mr. METCALF. I think I am getting the relationship. You are creating money, but you are doing it through a bank that is given the power to create money, or at least took the power to create money, whether they were really given it or not. I think this is something we had better look at, that in particular, because the Fed creates money, we know that. Are there any other comments on that?

Mr. VAN LEAR. Mr. Metcalf, the way we approach that is my company drives ATMs. We have 18,000 ATMs that people come to to make deposits and take out funds, and today, they do that usually with cash. They take out cash and they deposit checks.

As we move into the area of smart cards, we would expect the consumer to be able to put a smart card into an ATM and be able to move cash, if you will, from their account onto that card. That card, then, can be used to facilitate transactions such as were demonstrated here today through the use of a vending machine or on a transit or other types of applications.

We have facilitated the transaction, but it is really no different than if we had dispensed cash. There is no extension of credit. They are funds that have been moved from the account into a funds pool where they are reserved for the settlement of that transaction at a later date. So there is no funds creation, if you will, as a part of the movement of funds from a demand deposit checking account onto a smart card in the environment in which we are operating.

Mr. METCALF. In that case, I agree with you. When I take money out, then I am taking out money that I had. However, if it is a credit card, if you are going in there and borrowing money, you are creating money, and I think the best answer to that was the one who said, yes, we are doing that but we are doing that under the auspices of a bank which has the power.

I do think we should look at this area very carefully, though. Are there any other comments? I guess my time is up. Thank you very much.

Chairman CASTLE. Thank you, Mr. Metcalf. You sparked a discussion up here.

Mr. Chrysler.

Mr. CHRYSLER. Thank you.

Are your stored value cards equipped with a tracing mechanism so that law enforcement, after proper use of a search warrant and subpoenas, can track where the money came from and where it went?

Mr. CHAUM. I would like to answer that. The smart cards that we have developed are not, and I think that is the way it should be. If government were to insist that a low-value payment system, as I mentioned in my testimony—I hope you were here for that—were traceable, then that would represent an enormous erosion of the privacy that people have today in cash payments.

There is no more exposure to society in an untraceable chip card than there is in bank notes. In fact, I argued, and I hope it was persuasively, that, in fact, there is less exposure in an electronic system than in bank notes because there is no way to, for instance, accumulate value without that being known to a financial institution.

So it is more or less trivial to make a chip card that traces everything you do, every newspaper, every tram, every parking meter, and so forth. That is easy to do. But to make a system that allows people to have the same kinds of protections which they have an expectation of today, it is not as simple but it can be done and it can be done at essentially the same cost and with a very high degree of security.

Mr. CHRYSLER. Do you think crime will fall substantially?

Mr. CHAUM. No, and let me make this point very, very clear, if I can, and that is that by making a chip card protect privacy, you are not creating a more dangerous world than the cash that you are replacing. It is a safer world. So it is better to move to a chip card that has privacy in terms of abuse against society, in terms of protection of the individual and so on.

What would be a real mistake would be to move to an electronic payment system that is fully traceable, where you would be stepping backwards. You would be moving away from the kinds of pri-

vacy that people have an expectation of today into a totally transparent world.

I do not know if you have read about the panopticon. This is something that is devastating for the individual, and there is a great deal of literature to support that. So this would basically, to my view, undermine many things that this country stands for. It would create really the kind of world which many of us have fought to prevent.

Mr. CHRYSLER. I get your point. Will stored value cards be used primarily for transactions involving small or large sums of money, or both?

Ms. FISHER. We think that the card will be used primarily for small dollar purchases, but obviously, consumers with their banks will decide where it is most appropriate.

I would like to make one comment to your prior question, because the Visa stored value card product is one that is based on our existing set of products and it is auditable and traceable. Again, with due regard for the privacy principles that all banks have to safeguard, if it becomes necessary, working with law enforcement officials to trace something, we can do that with our system, and that is an important contrast, if you will, to what Dr. Chaum was talking about.

Mr. CHAUM. I would like to add something there. We are moving toward a new world with Internet payments, and there, since the transaction cost is dropping, what we are going to see is far more finer grain payments. So what may be an acceptable amount of privacy to forfeit today may become quite unacceptable in the future.

And similarly with the chip card, the transaction cost of payments is dropping, so what people are proposing to do in many countries is not just automatic toll payment at bridges but what is called road pricing, where you pay for every segment of the roadway that you use. I do not think many people would like to be followed around in their every single move.

Mr. CHRYSLER. I understand that.

Mr. CHAUM. Once coins and bank notes might become less accepted——

Mr. CHRYSLER. Your answer is consuming all of my time, if I can just cut you off. I am sorry. I just wanted to ask one more real quick question. At what transaction amount level will it be economically feasible for a business to purchase the appropriate equipment that will recognize these cards?

Ms. FISHER. I think that, to some degree, the cost will be determined by the level of regulation that is required. For example, if terminals have to print paper receipts for every transaction, that will probably not make it economically feasible at any level. So I think that it is somewhat dependent on how the parameters of Regulation E and the enforcement of Regulation E apply to this product.

Mr. CHRYSLER. Thank you.

Chairman CASTLE. Thank you very much, Mr. Chrysler.

We have a vote starting in about 13 minutes. It is one vote; it is a motion to recommit, but there may be some final debate and then a final vote on a piece of legislation, so we might use some time.

Perhaps we can move on to Mr. Watts' questioning and get that in before we have to break.

Mr. WATTS. Mr. Chairman, thank you.

I do not have any questions. I have an opening statement. Since I was absent during that time, I would like to request that this brief statement be admitted into the record.

[The prepared statement of Hon. J.C. Watts can be found on page 56 in the appendix.]

Chairman CASTLE. Thank you, Mr. Watts.

Any member is more than welcome to submit an opening statement. It will be made a part of the record if they submit it at any time during the day.

Ms. Maloney, do you have a question?

Ms. MALONEY. I would like to, if I could, put my opening statement in the record.

[The prepared statement of Hon. Carolyn B. Maloney can be found on page 57 in the appendix.]

My question is a security one. We had a great debate in an earlier meeting of this subcommittee over the security of ATM cards. What would be the security of these cards? If someone pickpocketed you, could they then just use these cards and it would be charged to you, or what is the technology on the security in the event of theft?

Mr. CHAUM. I believe that, as I was indicating earlier, the chip card can be better protection for the individual than with bank notes. Today, you can get several hundred dollars out of an ATM machine and if someone steals it, why, it is certainly gone.

With a chip card, for example, the one that the European Commission has sponsored, there is a small amount that you move to an in-cash which can be used without the entry of a PIN code, but then if you want to move additional funds from the reservoir into the in-cash, then you will have to enter a PIN code.

So there is the possibility to have much better protection for the individual. In fact, when we move to systems like this, they will probably be much smaller and nicer, it is actually up to the individual to choose the kind of security and protection they want. So they may program their device to require a PIN code for every transaction or to use a duress PIN code to display a smaller balance than is actually on the card, for instance.

Ms. MALONEY. But currently now in ATM cards, you need a PIN code for any withdrawal, so based on what you are saying, the PIN code would be more security for the ATM, because you were saying there could be a cash level before you go into a PIN card. Why is the security greater than an ATM card? You have a PIN code now with ATM.

Mr. CHAUM. Excuse me, I really was not comparing it to an ATM card. I was comparing it to the bank notes and cash.

Ms. MALONEY. Just the bank notes and cash?

Mr. CHAUM. Yes.

Ms. MALONEY. So it is very similar to the ATM in its security?

Mr. CHAUM. These cards are intended to replace bank notes and cash in low-value payments and they offer better protection to the individual consumer than the bank notes do because they allow the consumer to make it harder for people to steal their money.

Ms. MALONEY. Thank you.

Mr. VAN LEAR. Basically, with the ATM network, we would require the loading of value from an account to the card to require the PIN, so you would have the same security required in order to put funds from your demand deposit account onto the card.

We believe that the card will be used for low-dollar transactions and therefore there is no PIN required when you actually execute a transaction at a point of sale. So if you were to lose the card and you put $50 on it, that card would be available to anyone who found it to use it at the point of sale. It does not operate the way Mr. Chaum has outlined his, but that is an ATM transaction.

Ms. MALONEY. Thank you.

Chairman CASTLE. Thank you very much, Ms. Maloney.

I think we will break at this time. We have about 8 minutes until the vote. This may end up being two votes, so we may be gone for as long as 25 minutes or so before we can reconvene. I would like to reconvene. There may be Members who were not here who want to come in and ask questions, if their staff could alert them. We will be back as soon as the last vote is over, and I have a couple more questions I would like to ask, so to the extent that you can stay, we would appreciate it.

The staff could try the cards out and have their lunch.

We will try to reconvene about 5 minutes after the last vote, which I estimate to be probably in 20 or 25 minutes. Thank you.

[Recess.]

Chairman CASTLE. If we can resume, now that we have been well served with our stored currency or value cards. I discovered that Entenmann's actually has a little pie, which I did not know before.

We will continue with our questioning. As I indicated, some may not come back, some may, but Congresswoman Kelly is with us and we will turn to her for her questions.

Mrs. Kelly.

Mrs. KELLY. Thank you, Mr. Chairman.

I would like to address the panel. First of all, I want to thank you very much for coming in and testifying. I think what you are talking about, about the whole idea of handling money in the way that you are talking about, this electronic handling, is very exciting. It certainly is going to keep people's—one of the problems that I have with my husband is that coins in his pocket keep rubbing holes in them, in his pants pockets. You have to worry about those things when you are a housewife.

But I have to tell you, I am a little concerned about a couple of aspects here. I am concerned about things that are secure in terms of our money regarding money laundering. I do not see yet in the system of anything that I have heard about protections that would be there for people who want to launder money electronically.

I am also concerned about certain aspects of banking on the Internet, because to bank on the Internet, you have to go through a number of different systems. You are going one, two, three, because you are going through a lot of different systems to get across that Internet.

It seems to me there needs to be in place certain types of protections to protect us if we are going to do this kind of electronic banking and crediting. I do not care who wants to speak to this issue,

but I want whoever responds, I want a little time at the end because I have a follow-up question. So take it away, whichever one of you wants to jump in first.

Mr. COOK. Mrs. Kelly, let me respond. For the systems that we are working on, together with our bank partners, all use existing banks and existing payment methods, such as checks and credit cards, which provides substantial traceability. All the traceability protections which are in place today that prevent money laundering in those systems, the checks and credit cards are fully available in the systems that we are working on with our bank partners. So no reduction in the government's ability to prevent money laundering is involved in what we do.

Mrs. KELLY. Does anybody else want to talk about this vis-a-vis the Internet?

Mr. MELTON. Yes, just to answer the second part of your question. I would agree with Scott on the first part. He is entirely correct. These systems do go through banks and so all of the auditability is there.

We frequently start out talking about these kinds of questions assuming that there is a polarity or a binary relationship between privacy, on the one hand, and auditability, on the other hand. I would like to suggest that that is a polarity that with the new technology is not necessarily needed. There can be simultaneously privacy and, in cases of due cause or due process, there can be auditability.

Part of that comes from the technologies that apply to your second question, and that is if you are going through multiple points on the network, how do you know that you are safe, so to speak, at each point on the network? Two dual technologies. The first is the digital signature that every party to that transaction, yourself, there is a merchant, if there is a merchant involved, the bank, each one of you must have a digital signature that absolutely authenticates that you are who you say you are.

Then, based upon these known parties interacting together, you achieve privacy by wrapping your interaction with the known parties in non-breakable, non-openable envelopes that flow over this new frontier space. So while the space itself may not be safe, the envelopes through which your information passes are totally safe.

Mrs. KELLY. I see heads nodding in agreement. I find this a rather imperfect world and talking about things being absolutely safe concerns me a little bit.

I know we are going to follow up with a hearing, Mr. Chairman, on some of this technology, but I would like very much for people to address what technology there is with regard to security. I think it is very important that if we do not want to hold a separate hearing, that we address it here today, what technology there is available, because the security of these transactions is extremely important.

I am not so sure it is an appropriate place for government, because with the government regulations in place we may be micromanaging something that the market forces will micro-manage on their own. Nobody is going to give you their money to fly through the air if they are not sure that that money is going to be perfectly safe. So I am not so sure that is an appropriate spot for us.

I would like very much to put a plea in to you, Mr. Chairman, that we have a hearing, and I do not know what technology there is out there, but that we let people come and talk to us about that technology specifically. Is that possible?

Chairman CASTLE. If you would yield, I would suggest not only is it possible, I think it is very necessary. In fact, I intend to ask a couple of follow-up questions on this whole area of regulation here today. I think security is a very vital question, and while we may be safe in the systems which exist today, you can imagine if you have computers which can create value in some way or another, that somebody is out there—there are probably more people out there trying to break it than there are trying to create it, and that does raise certain risks.

We do have to make absolutely sure, probably much more so than we ever did within the banking system, that we are aware of any potential changes as they come along and what we can do to counteract that from a security point of view or a regulatory point of view or whatever it may be. I am not a strong regulatory person, any stronger than one has to be, but we certainly do not want a runaway system, either.

So I agree completely. In fact, I think at our hearing with the government officials, that issue should be addressed, and then we will see after that what further action we may need on it.

Mrs. KELLY. And it is possible we could talk to industry people, as well, on that.

Chairman CASTLE. Absolutely. This whole hearing is not pursuant to legislation we are pursuing. It is basically to educate this Congress about what is happening, and I think to some extent it is an evolving market and we should leave it alone, but at the same time, we need to be aware of the possible pitfalls and how we should react to them. It is really informational, what we are trying to develop here.

Mrs. KELLY. Thank you.

Chairman CASTLE. Thank you.

Following up on that, if I may, and I guess I will start with you, Mr. Cook, although Ms. Goff mentioned this, as well, and that is this whole area of regulation. You picked, by the way, the right Congress. This is the most anti-regulatory Congress that has been around in years. In fact, we just got rid of one regulation on the floor about 10 minutes ago. We are more into deregulating than we are into putting in new regulations, so when you make a plea that this is a nascent industry just being born, just trying to get off the ground and regulation could hinder it, I think you probably will find that falls on ears that will listen well to it.

I do not think that you would necessarily be aided by regulation, but what I just said to Mrs. Kelly really does concern me and I would hope would concern all of us, and that is when you deal in the world of computers, you deal in the world of being able to add value to a particular piece of plastic or use a computer chip or whatever it may be, you are dealing in something that becomes a little loose even in the minds of a lot of us, and could you potentially, instead of creating $20, create $20 million by the addition of a few zeroes, either by mistake or intentionally, and we need to be ready for it.

I was talking to a reporter on the way over to vote and I indicated to him that I am not for regulating in anticipation of what may happen any more than we have to, because, A) we do not know what will happen, and B) that can really mess up the market. On the other hand, I think more than ever before, we need to be ready to jump if the occasion arises. That is, if we find there are practices which are creating problems in the market or whatever it may be.

I just wanted to sound out your views. I think it is a potentially dangerous area. I just do not think it can be said to be wholly 100 percent safe from possible problems. I wanted to get your views, or both of your views, on where you think the regulatory aspects of this should come in, what they should be looking for, when they should be ready to enter into the fray or whatever it may be.

Mr. COOK. I agree with your instincts. This is not an area for government to go to sleep. At the same time, I think the things that were described by Mrs. Kelly in terms of some of the risk areas and the inherent incentives in the current players in the banking system to make sure those risk areas do not become real risks for consumers are so strong that if any of these techniques are to work, consumers must trust them.

Consumers are naturally not a trusting sort when it comes to new payment vehicles, so these things have to prove themselves in consumers' minds and they will only do that with an established track record of success where people are not losing their money unexpectedly. So I believe there are very powerful incentives in the marketplace to make sure these systems proceed exactly along the lines of eliminating or handling the kind of risks that you described.

At the same time, I think a government with the view that regulation is important when it is needed and can be an inhibition or restrain progress when it is not needed is an appropriate attitude, and hearings like this are a helpful way to stay in touch.

Chairman CASTLE. Ms. Goff.

Ms. GOFF. Yes, I would like to add, MasterCard International has been working on security on the Internet, along with Visa and Europay. I think that we would appreciate the opportunity to work with you and to have our specialist, while it is not my area of specialty, to have our specialist come and give testimony to your subcommittee and to anyone else who is appropriate.

We also have a subcommittee of our own International Operations Committee that is working on not only PIN but card holder verification methodologies, biometrics, and the evolution of how we identify card holders, which is another area that we think is very important to the privacy of the consumer.

So we would be happy to participate and support your work efforts, but certainly not to legislate at a time before the products have actually developed.

Chairman CASTLE. Thank you.

I want to start to wind this down but I have one more question that is sort of general in its nature. Again, it may come from my own lack of understanding, but I think it is important, and that is the Internet. Not only in the specific cards, but in some of the transactions, even the one we talked about in purchasing the flash

light, which Dr. Chaum's company is involved with, the Internet becomes, I guess, a key player in all this.

The whole history of the Internet is very fascinating, and the whole lack of any central ownership and all the different aspects that seem to exist are important. But is a lot of this dependent upon the Internet as it exists today? I mean, the Internet is taking on a life that is almost as big as television in this day and age. Everyone seems to be getting into it, and it goes all the way from business systems to pornography. There are fascinating articles about it.

It is this large, rather unmanaged, unowned thing that is floating around out there, and yet it seems to be at the heart of some of the systems that we are talking about in terms of invisible money or non-money money, as we have non-bank banks, the non-money money that we are starting to deal with here. I would be curious as to anything you are willing to share with respect to the significance of the Internet and the whole future of the Internet, and again, safety issues and just where we are going with the Internet as an aspect of this.

Mr. MELTON. To quote Ms. Goff's statement, I believe the figure that she used was that there is anticipated to be 100 million persons on the Internet within the next 5 years. The figures today say 30 to 50 million. Anytime there is an assemblage of that many people, we now have an active marketplace. Anytime there is an active marketplace with buying and selling going on, certainly there must be suitable payment instruments.

Already, there is a close working relationship developing between the engineers that created the Internet and the banks and the credit card associations. Just this past week in Stockholm, there was a worldwide gathering of all of the Internet Engineering Task Force. That is, the engineers that kind of get together on a collegial basis and decide what to do.

At that meeting were representatives from most of the people that you see in front of you, including MasterCard and Visa, talking about the very problems and the opportunities that we are talking about here today. There is a coming together. There is a consensus developing on how we shall deal with many of these problems. We have great faith that these problems are solvable and they are on their way to not only not being problems, but there being real opportunities for a reduction of cost to the consumer with greater options for the consumer to buy things. Thank you.

Chairman CASTLE. Let me turn to Mr. Flake and see if he has any follow-up questions he would like to ask.

Mr. FLAKE. Thank you very much, Mr. Chairman.

Let me just make a statement and then just ask for a response to it. If people who log on to the Internet are localized geographically and thus subject to a particular set of national laws, the traffic that they create on the Internet is not very obviously anywhere at all.

When global digital cash becomes a reality, tax men and women will have their work in deciding how to assess assets that might be stored on a different computer in a different country every day, even assuming they could ever find the assets or the computers. And for those who choose to evade tax actively, the opportunities

offered by the Internet would be certainly tempting, just as they already are for pornographers and others.

The question is, how will the government be able to regulate commerce and banking on the Internet, given these transactions can occur in any number of countries and there are different policies as it relates to how they regulate their commerce? Does anybody want to take that? Dr. Chaum?

Mr. CHAUM. Thank you. It seems to me that the Internet and chip cards are really properly thought of as part of the same phenomenon generally. We need to take an integrated solution to all of these electronic means of payment.

The answer to the issue of tax evasion is the same as the answer to the issue of money laundering and so on, and that is simply that money will live in bank accounts and only be withdrawable into these electronic forms in limited quantity. There will be only a limited amount of money which you can store on a card, only a limited amount of e-cash which you can withdraw from your bank and have in your work station.

In that way, this money will be no more a problem from the point of view of the tax collector, the money laundering chasers, the drug enforcement people, or whoever than paper money is today. In fact, as I like to believe, and I hope is represented in my testimony, at least, that that will be less of a problem than bank notes and coins are today in that regard.

If these electronic means of payment are viewed as a low-value cash replacement, then they should only be thought of as a way to improve enforceability of all kinds of regulation.

Mr. FLAKE. When you talk about limited amounts, obviously, with our reporting functions to the Federal Government by banking entities now of cash that equals or exceeds $10,000, how would you set a limit in this kind of situation? Are you talking about an actual dollar limit that would be set by some entity for which there would be a regulating body that would oversee it, or is this going to be a limit that is determined by whoever has charge of that particular segment of this industry? Who sets the limit and who regulates it?

Mr. CHAUM. There are a lot of limits in place today and they have already been set. Those probably are adequate. I do not really think there is a need to bring the limits which are set lower, but the technology, of course, will reduce the cost of administering reporting and it will allow the limits to be set lower than they are today, which is just another way that this kind of technology can still protect the interests of society better than paper money.

Mr. FLAKE. Are the maximums on those limits determined by the actual kinds of transactions? How do you determine what your outside limit is? What becomes unreasonable? What creates the possibility for some type of corrupt activity? How do you set that outside limit that you know is secure enough to protect that person who has monies in this system?

Mr. CHAUM. I think that the limits which are set today are quite——

Mr. FLAKE. What do those limits look like, maybe Visa or MasterCard?

Ms. FISHER. If you are talking about the stored value card, for example, as one example——

Mr. FLAKE. Yes.

Ms. FISHER. My point would be that banks, in conjunction with their customers, will decide what is appropriate. To some extent, you are relying on consumers' good judgment, and I think consumers have demonstrated good common sense in determining what they feel comfortable with having in a stored value card that they might lose, just as they make the decision every day, how much money do I take out of the ATM this week that I feel comfortable having on my person. Or similarly, those kinds of decisions that you make every day about how much cash are you going to carry around.

I do not think the government should set these limits. I think these would be limits that banks, in conjunction with their customers, would deem appropriate from what the marketplace would like to see made available to them.

Mr. FLAKE. It is not just a consumer issue. I think all of us understand that as you develop systems, there is someone developing a counter-system that will allow them to be able to access the means of being able to take advantage of other people. I mean, when I get a $3,900 phone bill on my car telephone, in spite of the fact that I have a PIN number, there is always somebody out there aggressively operating the same as you do in terms of trying to create a positive means of being able to do business, there is someone out there doing business that is corrupt and they are looking for ways to see if they can take advantage of it.

So I guess a part of our concern will have to be what kind of safeguards you put in, if you need any at all, and maybe your maximum limits are of such nature that you can control it. But I am not sure, given the safety factors that we have seen, whether it is the cellular phone industry or other industries, that there are people who are going to find ways to take advantage of this.

If there are no other comments, I yield back my time.

Chairman CASTLE. Thank you, Mr. Flake.

At this point, I would like to wrap up the hearing. Is there anything that anybody has heard that they feel should not go unrebutted or unstated before we close? Mr. Van Lear?

Mr. VAN LEAR. I am not going to rebut something but I think I would offer an observation, and that is I think the role of government is not just to provide the oversight, but I think in this particular case, government really should be looking at taking advantage of some of the technology that we have here. We have an opportunity to do things that I think the government wants to do and should be done, and in particular, I will speak to the area of remote distribution.

In the entitlement programs that are in place today, the cost to the recipient for being able to take that entitlement check, which is typically in the form of the check, and have that check cashed and then do bill payment is an extraordinary amount of money. Most of the people who are on those entitlement programs are nonbanked people.

We have technology, and it is running in the State of Delaware today, where we can cash a check at an ATM to the penny. We

have technology through some of the products that are offered by people at the table here who, in fact, can provide bill payment through those ATMs for non-bank people. If there is an incentive for us to do that, those kind of products can be delivered and the beneficiary of them will be the taxpayer, because it will be a lower cost solution, and the beneficiary will also be the people on the entitlement programs themselves.

So I think government needs to take an active look at what this technology can do for them in the various areas of entitlements and electronic benefit transfer and do that in an aggressive role. There are a number of partners, such as our organization, who are more than happy to do that.

Mr. FLAKE. Let me just offer one reaction to that, and that is that I agree with you wholeheartedly, it is a great thesis. The problem is that in many of the poor communities where people receive the benefits of entitlement programs, there has not been a historicity of institutions and entities wanting to provide the same kind of access, so that you do not have banks, you do not have ATM machines, so that the question becomes, even though this is probability, and I tend to agree with you, this is probably safer. It keeps people from worrying about having checks stolen and so forth.

How do we guarantee in those communities that are, in effect, what many in various industries would consider poor communities and therefore do not provide a level of opportunity for access to those services? How do we guarantee that those services will be available to them? It would solve a myriad of problems for us if, in fact, it worked the way you suggest it would, but I just wonder if it really will. Will these communities and persons in those communities still be left out of the process and left out of the loop?

Mr. VAN LEAR. I think you have two issues there. One deals with the ability for the current and past technology to be able to deliver this kind of service. In the past, in order to cash a check or to put a deposit in an ATM, you were required to have an account at a financial institution. The financial institution had a cost associated with that, and so therefore the unbanked, if you will, were unbanked because of the fee structure that was associated with banks being willing and able to do that at a reasonable fee.

If the technology would provide for the equipment to do the check cashing without the involvement of an account on file with that institution, and that can be done, then there is a reason for the deployment of those technologies to take place in locations where they have not taken place to date.

It is not a brick and mortar issue. It is a matter of being able to deploy technology that today can effectively take a payroll check or an entitlement check or a government check and basically cash that for someone without an account. That service can be developed and it can now be delivered. It could not have been delivered years ago, simply because the ATM was limited in its ability to perform that function.

So I think there is an incentive and there is an opportunity here, but it is going to take people working together to do that and I just think that government ought to take a proactive role in looking at what those opportunities are.

Mr. FLAKE. I think some of us would want to do that for an additional reason. That is, many of the people in those communities now pay about 20 percent just to cash that check. I think I would be more than willing to talk, have some more discussions with you and any members of this particular panel, because I can see some long-term positive benefits from it, and hopefully, working together, we can resolve how those individuals who are living sort of hand-to-mouth in some instances will have more of their own resources to live with by virtue of the fact that the technology has been brought to those areas where they live.

Thank you very much. I appreciate your answer.

Chairman CASTLE. Mr. Melton, did you want to answer that?

Mr. MELTON. Yes. I was just going to add to the comments that were just being made. While ATMs certainly are capable of providing the kinds of services you are talking about, there are now many locations developing where we do not even need the cost of an ATM. The very kind of equipment you see sitting on the table down at the end here, where we are talking a few hundred dollars, now is capable of doing the same kind of ATM-like functions.

This kind of equipment ends up being at the grocery store or at the kinds of service establishments without much of an overhead burden to that store. They frequently need the equipment anyway for doing other kinds of transactions and these same kinds of things can be done through that equipment with almost zero additional cost.

Chairman CASTLE. Is there anything else anybody would like to add? Mr. Cook.

Mr. COOK. Let me just add a description of an additional benefit area of what PC technology can bring to people's finances to add to the benefits that have been mentioned already.

Probably the best illumination of this is to describe a story which points up how complex financial matters have gotten for people in this economy. It used to be so simple. When you wanted to refinance your house, there was one kind of mortgage. You could compare interest rates and know which one was the best. Today, there are so many different variations and types and styles and rates and different ways they work, which have all been designed to give customers more choice and pick the best one, but it is bewildering today. The same thing is true in mutual funds and investing and saving issues.

Just one simple description of that was brought home to me when a member of the press, who I was describing what we were working on last year, he said, let me tell you about my recent experience in refinancing my house. He had done this before. He was knowledgeable about how. He called his banker and said, I am trying to minimize my cost over the next 5 years, at which point I will trade up to a larger house. Which of your mortgages do you recommend?

The person at the bank described the various mortgages and then recommended one. He said, well, that is not the lowest-cost one. The banker said, what do you mean that is not? The customer said, well, I am using the Quicken mortgage calculator. We have this simple mortgage calculator in Quicken. He said, this other one that you are not recommending is, in fact, lower cost. For a few

minutes' time on the part of that customer, he saved himself hundreds of dollars.

I later ran into the vice chairman of the bank at the bank this person was dealing with and I mentioned this story, and I did it very sympathetically, knowing how hard it must be to assure consistency and quality across hundreds of branches and thousands of bank employees, or any kind of employees in financial products which are as complex as they are today. And he said, no, Scott, it is not difficult, it is impossible.

So we literally have a financial system which, in its great creativity, has built great products of all kinds, but helping poor consumers, or helping any consumers make the decisions about which ones are right for them, there has not been a similar advance in the art. We think that computer technology of the type we have talked about today will help people make sounder financial decisions that literally will save them hundreds of dollars a year, and upon things like retirement could make a difference of hundreds of thousands of dollars a year. That is, I think, part of the promise of these technologies.

Chairman CASTLE. Let me thank all of you very, very much. We really appreciate this hearing. I think we are breaking new ground here in terms of hearing about the use of the—I don't like the expression of non-money money. I never liked non-bank banks, so want to be careful about that. [Laughter.]

But the concept of using computer technology in general, the Internet, the stored value cards, the different way of being able to purchase things that we have just not been exposed to before.

I think we have heard some very interesting things, one which clearly is, let the market form itself, and that is correct. If the consumers are not going to take to it, it is not worth much, and you cannot regulate it out of business before it gets there so we need to pay attention to that.

A number of us raised questions about security. You did, as well, in many instances in your statements, and we need to be also, I think, concerned about that.

Regulation remains an issue that we are going to discuss later in September. I remind you of what I said in my opening that Mr. Diehl had said, and he was in the back of the room during most of this hearing. He had indicated that, left alone and unregulated, the market might produce an electronic "Tower of Babel" with no single standard of technology and many opportunities for law avoidance and criminal transactions. An overreaction? I do not know. This is something we have to find out.

But in any event, I think we are all aware that the world of computers changes much faster than the paper world ever changed, and for that reason we have to be anticipating and ready for all this.

Here at the end, and at some point in the middle of the testimony, we heard about potential services to those who cannot afford all of the upscale computer links or whatever it may be, but there may be other values that could be added for them that could, in fact, relieve them of some of the burdens which they face today that perhaps we do not think about a great deal, such as check

cashing charges and loss of stamps and other things that may happen. I think that is valuable, too.

We have an accumulation of lights and pies and cards and all manner of things as exhibits of what can be done with all this, and we appreciate that, as well.

We do not have legislation in hand. We do not have regulations in hand. This hearing was not for that purpose, nor are we developing any, I might add. This hearing was not to get that process started. It was to learn more about what you are doing.

I address this to the panel but also to the other individuals who are here who are interested in this for various reasons. We are very interested in developing whatever knowledge we can. Therefore, if you have knowledge or articles or something that you think might be helpful, my staff would be glad to read it. I am not sure that Mr. Flake and I have time to read it all, but our staffs certainly can, and they are up here with us and we appreciate all the good work that they have done because we want to absorb as much as we possibly can.

We do not want to interfere with what you are doing at all. We want to encourage you. We want to encourage you to develop new products in the marketplace and save people money, help them with their retirement, as Mr. Cook has talked about, whatever it may be. On the other hand, we want to make sure that we are carrying out our responsibilities as well as we can, also.

So we appreciate you being here today and answering questions. There is a possibility that when we get through with all of this, we may have additional questions which we would like to be able to submit in writing to one or more of you if you would be kind enough to look at those and answer them. That may or may not happen.

That is all I have to say in conclusion. With that, again, we thank you, and we stand adjourned.

[Whereupon, at 12:59 p.m., the hearing was adjourned.]

APPENDIX

July 25, 1995

The Future of Money hearing - July 25, 1995, 10:00 a.m.,

Room 2128 Rayburn House Office Building

Hearing to explore the impact of new technology on future payment systems, money supply, privacy issues, security and regulatory compliance issues.

Chairman's Introduction:

The subcommittee will come to order. Welcome to the House Banking and Financial Services Committee, Subcommittee on Domestic and International Monetary Policy Hearing on the Future of Money. Again, this Subcommittee is positioned to have initial jurisdiction of an important area of public policy.

The Future of Money contains the potential both for great commercial promise and for enormous risk of undermining the system of exchange and the administration of justice. This is true whether the media of exchange enter electronic commerce using computers linked into networks or via computer chips embedded in cards or other devices.

At a recent hearing on the Dollar Coin before the Senate Banking Committee, Philip Diehl, Director of the Mint, noted that the state of affairs with Electronic forms of money was analogous to the situation before the Civil War when local banks issued their won paper money. He foresees that left alone and unregulated, the market may produce an electronic "Tower of Babel", with no single standard of technology and many opportunities for law avoidance and criminal transactions. We will begin to explore these emerging "Third Wave" forms of currency and begin to define the appropriate role of the federal government with reference to this evolving technology. This will not be accomplished in a single day or one hearing. This morning we will hear from a panel of six expert witnesses, all from the private sector. With their assistance we will begin to consider some of these vital issues. At a later hearing, governmental entities with responsibilities in the management of the integrity of our monetary system and others with responsibilities for the enforcement of laws relating to it, will testify. At that time we will consider in greater depth public policy issues raised today.

With more than two trillion dollars currently moving electronically each day between U.S. institutions, the safety and security of this system is not to be taken lightly. Basic requirements are clear. Payment instruments must be widely accepted, convenient, cost effective, safe and confidential to assure wide usage. The legitimate law enforcement and public policy interests of the government must also be recognized. Cooperative efforts between banks as an industry and between banks and the government have made the current payment instruments successful and widely used, and if these precedents are applied in future payment mechanisms, they may be made similarly successful.

We are indeed fortunate to have before us some of the pioneers of new electronic payments technology to discuss their creations and the implications of its implementation.

They are:

David Van Lear, President, Electronic Payment Services

Dr. David Chaum, Chairman and CEO, DigiCash Inc.

William Melton, Chairman and CEO, CyberCash Inc.

Rosalind L. Fisher, Executive Vice President, Visa USA

Heidi Goff, Senior Vice President, MasterCard International

Scott Cook, Chairman, Intuit Inc. - Owner and developer of Quicken, the leading personal finance and home banking software.

STATEMENT OF FLOYD H. FLAKE BEFORE THE HOUSE SUBCOMMITTEE ON DOMESTIC & INTERNATIONAL MONETARY POLICY JULY 25, 1995

I thank you, Chairman Castle, for convening this important hearing, and I congratulate you for your diligent effort to explore various issues as they relate to the future of our money supply. As you are certainly aware, our committee is beginning a process that will examine the United States' payment systems, and the new technologies that might change traditional means of monetary exchange. We are, however, obliged to examine the government's role in the context of potential social, tax and criminal implications of these new payment systems. Knowing

this, it is imperative for the committee to look at the efficacy of the various programs on their merits, and to resist the undoubtedly exciting nature of these hearings. Consequently, I look forward to our future deliberations on this subject.

Briefly, I will outline some of my concerns. With respect to stored value cards, I recognize that these cards will definitely be a plus to consumers, especially as the advanced technology is further developed. However, will the cards maintain anonymity in financial transactions, and how secure will the smart cards be?

Another concern is the availability of this technology in poor communities. Presently, there is a

dearth of banking and financial services in minority and poor communities due to redlining. What will this committee do to ensure that this does not occur with new payment systems. Given the historical unavailability of high technology in poor communities, I believe that it is this committee's responsibility to ensure the universal availability of these new services.

Finally, Mr. Chairman, electronic banking presents the same concerns with the additional prospect of tax evasion and money laundering activity. Moreover, how will people know legitimate online services from fraudulent ones? With more than 30 million current users, and a projected 200 million users in the future, there are cyber-criminals who cant

wait to use the Internet for ill gains via phony home pages. Obviously these are vital public policy issues, and I look forward to commentary from our witnesses and other committee members.

REPRESENTATIVE EDWARD ROYCE

OPENING STATEMENT

SUBCOMMITTEE ON DOMESTIC & INTERNATIONAL MONETARY POLICY

July 25, 1995

THANK YOU, MR. CHAIRMAN, FOR HOLDING THESE TIMELY AND IMPORTANT HEARINGS. I AM EAGERLY LOOKING FORWARD TO THE TESTIMONY OF THESE WITNESSES REGARDING HOW DEVELOPING TECHNOLOGIES IN THE PRIVATE SECTOR ARE PUSHING THE ENVELOPE OF HOW WE HANDLE FINANCIAL TRANSACTIONS, COMMERCE AND EVERYDAY PURCHASES.

THE TECHNOLOGY THAT WILL BE DISCUSSED TODAY IS CERTAINLY AWE INSPIRING AND TO SOME A BIT FRIGHTENING. WITH THE EMERGENCE OF **E-MONEY, SMART CARD SYSTEMS AND DIGITAL CASH** AS VIABLE AND SECURE ALTERNATIVES TO ORDINARY MONEY A MAJOR STEP WILL BE TAKEN IN THE DIRECTION OF FULLY DIGITIZING CURRENCY.

CONSUMERS WILL LITERALLY HAVE AT THEIR FINGERTIPS ACCESS TO MAKE PURCHASES OR FINANCIAL TRANSACTIONS FROM ACROSS THE WORLD AT AMAZING SPEEDS. BUSINESSES AND BANKING INSTITUTIONS WILL HAVE A MORE SOUND AND

ACCURATE MEANS IN WHICH TO IDENTIFY AND APPROVE THESE TRANSACTIONS - AND ALL OF THIS UNDOUBTEDLY WILL SAVE MILLIONS OF DOLLARS A YEAR IN PAPERWORK. THIS IS TRULY USING TECHNOLOGY AND PRIVATE SECTOR INNOVATION TO THE BENEFIT OF OUR SOCIETY.

UNFORTUNATELY, AS IS SO OFTEN THE CASE, WITH ADVANCEMENTS COME INCREASED RISK. INCREASED RISK IN THE FORM OF FRAUD, THEFT AND POTENTIALLY VAST MONEY LAUNDERING SCHEMES CARRIED OUT BY THOSE WHO WOULD SEEK TO EMBEZZLE FROM AND MISUSE DEVELOPING TECHNOLOGIES.

I UNDERSTAND THAT AS COMPANIES GO FORWARD WITH THESE INNOVATIONS IT WOULD BE UNWISE AND EVEN HARMFUL TO OVERREGULATE THE PROCESS. I HOPE THAT OUR WITNESSES TODAY WILL HELP EASE THE CONCERNS OF SOME IN LAW ENFORCEMENT, AS WELL AS CONCERNS OVER SAFETY AND SOUNDNESS AS THE MARKET PROCEEDS TO BRING OUR DATED PAYMENT SYSTEM INTO THE 20TH CENTURY.

REPRESENTATIVE JACK METCALF

OPENING STATEMENT

SUBCOMMITTEE ON DOMESTIC & INTERNATIONAL MONETARY POLICY

July 25, 1995

THANK-YOU MR. CHAIRMAN,

AS ONE WHO HAS WATCHED HISTORY, IT IS FASCINATING TO WATCH A NEW WAVE OF TECHNOLOGY COME TO THE FOREFRONT OF OUR SOCIETY, I MUST SAY IT IS OBVIOUS OUR WORLD IS CHANGING RAPIDLY, ESPECIALLY IN THE COMPUTER AND INFORMATION SERVICES ARENA.

AS I SEE THIS NEW ERA OF ELECTRONIC MONEY, SMART CARDS AND CYBER-CASH THERE ARE A COUPLE OF AREAS I MUST INTERNALIZE. IT IS OBVIOUS THE MARKETPLACE IS DICTATING A NEW METHOD, A METHOD WHICH STREAMLINES EVERYTHING FROM HOW WE PAY OUR MORTGAGE TO HOW WE BUY A COKE.

YET, GOING HEAD-LONG INTO A NEW TYPE OF ELECTRONIC MONETARY SYSTEM BRINGS WITH IT MANY QUESTIONS. QUESTIONS LIKE PRIVACY AND SECURITY, COMPETITION IN THE MARKETPLACE, ASSURING THE INTEGRITY OF TRANSFERRING MONEY AND ASSETS, GUARDING AGAINST ILLEGAL ACTIVITY SUCH AS MONEY LAUNDERING AND TAX FRAUD, AND ONE OF THE MOST IMPORTANT ASPECTS I SEE IS THE POTENTIAL FOR SYSTEMIC RISK. THAT IS A COMPLETE BREAK DOWN OF FINANCIAL MARKETS AND THE FINANCIAL SYSTEM AS A WHOLE.

EVEN THE CONGRESSIONAL RESEARCH SYSTEM MENTIONS THIS AS AN AREA OF CONCERN. AS FINANCIAL TECHNOLOGY HAS INCREASED AND FINANCIAL TRANSACTIONS ENTER HYPER-SPEED, THIS CAN ASSIST IN INSTABLE SITUATIONS LIKE THE 1987 STOCK MARKET CRASH OR THE DERIVATIVE LOSSES COMPILED BY BARINGS BANK.

I AM EXTREMELY INTERESTED, IN HOW THESE AREAS WILL BE ADDRESSED BY THE MARKETPLACE AND BY GOVERNMENT. AND I LOOK FORWARD TO YOUR FEELINGS ON THESE ISSUES.

THANK YOU, MR. CHAIRMAN.

REPRESENTATIVE J.C. WATTS, JR.

OPENING STATEMENT

SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL MONETARY POLICY

HEARING ON THE FUTURE OF MONEY, JULY 25, 1995

Good morning. I would like to thank the witnesses for being here and the Chairman and his staff for holding this hearing.

As the "information highway" emerges into the markets of home banking and electronic commerce, I think this is a ripe opportunity to examine a multitude of issues -- banking industry and consumer concerns, privacy issues, law enforcement and the role, if any, of the government as regulator. I look forward to hearing your testimony and again thank you for being here today.

CAROLYN B. MALONEY
14TH DISTRICT, NEW YORK

1504 LONGWORTH BUILDING
WASHINGTON, DC 20515-3214
(202) 225-7944

COMMITTEE ON BANKING AND FINANCIAL SERVICES

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

DISTRICT OFFICES

110 EAST 59TH STREET
2ND FLOOR
NEW YORK, NY 10022
(212) 832-6531

28-11 ASTORIA BLVD.
ASTORIA, NY 11102
(718) 932-1804

619 LORIMER STREET
BROOKLYN, NY 11211
(718) 349-1260

Congress of the United States

House of Representatives

Washington, DC 20515–3214

OPENING STATEMENT
"The Future of Money"
July 25, 1995

Thank you, Mr. Chairman.

I look forward to listening to testimony from today's panelist. It appears that we are embarking upon a brave new world in which the need for cash will be virtually eliminated.

Prepaid cards may eventually provide more security than cash.

But as we enter this new world, I hope we find ways to include all Americans. These new technologies may prove to be out of reach for the poor or the elderly. The testimony we are about to hear indicates that younger Americans adapt more easily to the new technologies. They are more likely to use ATM machines, bank by telephone and use computers.

Although the number of Americans who own computers has grown exponentially, they are still too expensive for many. And although the Internet is relatively cheap, it still remains outside the reach of many.

On the other hand, the possibilities opened up by the new technologies are fascinating -- prepaid cards will help eliminate the annoying problem of searching for exact change on buses, at parking meters and at the laundromat.

In many neighborhoods of New York City, few people have bank accounts. For that reason, check cashing offices have flourished. They charge sizable fees to cash checks for people who have no banks. Those who cash their checks at these places have no place to keep the resulting cash. They become walking targets for thieves who prey on the vulnerable. Prepaid cards with good security may be a solution to this problem.

I look forward to learning more about these new possibilities.

Thank you.

Electronic Payment Services, Inc.
1100 Carr Road
Wilmington, DE 19809

ELECTRONIC PAYMENT SERVICES, INC.

Submission In Support

of the

Remarks of David M. Van Lear

to

United States House of Representatives

Committee on Banking and Financial Services

Subcommittee on Domestic and International Monetary Policy

Hearing

The Future of Money

July 25, 1995

EPS was formed a little more than two years ago as a result of a number of emerging trends within the banking industry. The growing and rapid consolidation of the banking industry has led EPS' owners to conclude that they need to provide consistent services to their consumers over a broader geography.

The cost of research and development for these new financial services have reached staggering numbers. As a result, very few financial institutions can individually continue to make the level of investment that is required to provide new financial services. Therefore, a company like EPS which combines the resources of a number of large regional financial institutions is better able to amass the investment capital required to develop new financial services and enhancements to the current electronic payment systems.

Over the past twenty years, our industry has developed services using electronic means which provide consumers with a never before known level of 24 hour, seven day a week access to their funds. As a result of this convenience, and the reliability of our systems, the public has developed great confidence in our services. Due to this confidence, the consumer is asking for even greater levels of service and convenience. We are at the threshold of providing the full range of financial services directly to the home, which according to market research, is where consumers would like them, EPS is extremely interested in being a provider of these new levels of services for the consumer. The key requirement of a payment system process is systems integrity---without this, there would be no consumer confidence and thus no commerce.

Let me give you some history on the development of the existing levels of Electronic Commerce and the steps we in the banking industry have taken to provide system integrity. Electronic commerce is dependent on several major factors. First, the establishment of a communications network which allows parties to communicate instantaneously with each other. Second, the development of computer systems which allow for the swift accurate verification and authorization of transactions.

In addition, there are a number of major issues which provide the base upon which public confidence is built. First, there must be an assurance that the transfer of value will occur safely based on financial soundness of the party settling transactions. Second, the system must provide a reliable means

of accurately authenticating transaction requests by a consumer and assuring all parties that the transaction is valid. Third, there must be system security which assures all participants that only the appropriate parties will have access to sensitive personal and business information and the funds to be transferred. Lastly, there must be protection of privacy for the consumer, the bank, the merchant or any other party to a transaction. All of these factors are required to provide the system integrity and reliability which we have built into our current services.

Electronic commerce takes place using some form of electronic processing for the exchange of value. United States coin and currency are the means of value exchange which have been authorized, sanctioned and controlled by the government. The government's role is to preserve and control this means of value exchange.

Late in the 19th century, with original development of commercial uses of electricity to provide communications, the very first example of electronic commerce was developed through wire transfers. An example of this type of commerce was the Western Union Telegraph Company service where an individual delivered currency to a Western Union office and an instruction was sent to another location to disburse an equal amount of currency to a party that was able to identify himself properly at that other location. After such authentication of the party was established, cash was delivered.

In this example, there was no banking environment. Western Union, a communications company and not a bank, provided the services. Assurance of payment was not provided in any fashion other than the financial stability of that company. Security was provided because it was a privately controlled single purpose transmission facility used to send messages and these kinds of funds transfers. Authentication was provided by a signature at the other end of the transmission to verify that the party who received the funds was the intended party. Because this was a dedicated, privately controlled communications line, it was not shared with the public and therefore transactions were private.

After World War II there was a tremendous growth in consumer banking in the United States. Individuals who had never had checking or savings accounts before, began to use financial institutions for this purpose. The use of checks became wide spread, but payments by check were

cumbersome and there was no assurance that a check would be honored. In the mid 1950's a new product, a travel and entertainment card, began to be used by individuals, particularly those who traveled on business.

As computers were developed and began to be deployed by banks in the early 1960's, the ability to maintain information and to quickly check records about individuals and their credit histories became substantially greater and more effective. During the middle 1960's these improvements in computing technology fostered the creation of a new financial product, the credit card, which then began to be issued to large number of consumers. A credit card simply represents a pre-approved extension of credit by a financial institution to a customer. The advantage to the merchant was a higher level of assurance of payment for goods than checks as the issuer of the card was guaranteeing payment.

When a credit card is used to purchase goods and services, the merchant will obtain an authorization for such a transaction which guarantees payment. The merchant's bank then collects the funds from the consumer's bank. This system became more electronic as newer communications systems and electronic terminals capable of capturing information over the telephone lines where developed. Additionally, associations of financial institutions, such as MasterCard and Visa ,were formed to establish rules and methods for conducting inter- bank transactions between the issuers of cards and the merchant banks who acquired transactions through their merchant customers. These associations helped to provide standards for authenticity, security and to add certainty and reliability to the system.

Now when a consumer presents a credit card to a merchant, the merchant will swipe the credit card through an electronic terminal and receive an electronic authorization of the transaction. The transaction is then submitted to the merchant's bank who will collect the funds from the consumer's bank. The transaction is completed by depositing those funds into the account of the merchant.

What issues are relevant to this process? First, all transactions are occurring within the banking system and, through regulatory oversight, the safety and soundness standards are applied to the various banks which provide the settlement functions to assure payment. Second, authentication of these transactions is handled by a signature of the cardholder compared to the

signature on the card. In some cases today, a photo of the cardholder is actually on the card and can also be used for identification. The status of the account is checked by the bank which issued the card to the consumer. Various status messages are sent by the cardholder's bank back through the system to the merchant terminal, either approving or declining the transaction. Security is provided since the transactions are maintained within the banking system. Consumers and merchants use banks which operate within the card association rules which have been accepted by contract. Privacy is provided because these are contained, not public systems, and there are strict system rules on information disclosure to third parties.

Following the introduction of credit cards, the next major advance in technology was the development of a machine that could perform many of the functions of human tellers. Beginning in the early 1970's these automated machines, ATM's, began to be deployed by banks who then issued access cards to their depositors enabling them, for the first time, to obtain electronic access directly to the funds they had placed on deposit with a bank. The consumer could now get cash and make deposits through the ATM machine at any time of the day, even when the bank offices are closed.

In a cash withdrawal through an ATM, currency is dispensed through the ATM operated by the customer's own bank. All transactions are between the bank and its own customer. Payment assurance is through application of the safety and soundness standards the bank. Security is supplied by the use of an electronic signature, an encrypted personal identification number or code, which is used by the cardholder to identify, verify and authenticate the transaction request. Since the entire transaction is conducted within the customer's own bank, monitoring of the various lines and systems provided security. This is like a private communications facility. The authentication is provided because the bank authorizes the transaction against the funds that are on deposit and verifies the request by the use of the personal identification number or PIN. As to privacy issues, since the bank controls all of the information exchange between the cardholder at the machine and itself, there is no privacy concern. This same system is used for electronic cash deposits through the ATM. In this particular case, all of the protections that apply to a cash withdrawal are applied to a cash or check deposit.

In the evolution of electronic commerce, the next major development was the formation of what is known as ATM networks. In these situations, a bank or a third party data processor acts as a switching point for various financial institutions which are linked to a network computer. These connections allow the exchange of information between banks. Generally these networks operate with a common name or logo. In EPS' case, the trademark we use is MAC, which is an acronym for MONEY ACCESS CARD and MONEY ACCESS CENTER. Other major networks you may be familiar with are known as HONOR, MOST, NYCE, STAR PULSE and TYME. There are approximately 60 ATM networks in the United States today.

With an ATM network, a customer of one bank is able to use an ATM operated by a different bank. Money dispensed through the ATM comes not from the customer's own bank but through the ATM of the second bank. The transfer occurs by the exchange of information from one ATM to the network switch to the customer's own bank.

At the end of each day there is a settlement among the banks for the exchange of funds. In network transactions, we see that all transactions continue to take place within the banking system, providing assurance of payment safety. Where processing is provided by third party processors, such as EPS, the processors themselves are examined by the various federal regulators for system integrity. Authentication of transactions is provided just as in the previous example by review of customer records and through the use of the electronic signature, the PIN, which verifies the request of the cardholder and validates their transaction request. Security is also provided in such fashion through the monitoring of lines and systems and the use of dedicated leased communications lines. Encryption or coding of the PIN or the electronic signature occurs at the ATM to prevent unauthorized capturing. This encryption flows through the system to protect the cardholder. As to privacy, we have current federal laws that relate to bank exchange of information and agreements between banks networks and processors of confidentiality.

As all of these systems developed in the middle 1970's through the early 1980's it took a period of time for the average consumer to get used to using the systems and to develop the required confidence. However, once the convenience and the reliability of these systems was established, consumers

desire to use these kinds of financial services for additional uses has expanded. The largest growing number of electronic transactions today is in the area of debit point of sale transactions. In this case, that means taking the card that you know as your ATM card to a merchant, (such as a supermarket, a gas station, a convenience store or some other store and using that card) to make a purchase in place of using cash, or a check or credit card. The transaction works very much like a credit card transaction with a few exceptions. In this instance the ATM card is given to the merchant for the purchase. The merchant uses a higher grade transaction terminal and swipes the card in the terminal which reads the information, the customer enters his PIN and then the terminal routes the requested transaction through the ATM network back to the customer's bank for authorization against the customer's demand deposit account. The funds, once approved, are transferred from the customer's bank to the merchant's bank and placed on deposit there.

Again, we have a situation where these transactions are fully within the banking system and safety of payment is assured. The third party processors who provide services for merchants, like EPS' Buypass subsidiary, are also examined by the federal regulators for system integrity. Both the consumer and the merchant maintain bank accounts, and the funds are transmitted inter-bank within the payment system. Authentication is provided just as at the ATM by the use of the electronic signature or PIN to verify and authenticate the request. Security is provided because the PIN's are sent through the system on an encrypted basis. Further, the PIN pads and terminals in use today have been made tamper proof. Should someone attempt to do something with them to capture these PINS, the terminals and PIN pads would not function properly. Dedicated communication lines are also often used, particularly by larger merchants. In the area of privacy, we have network rules which require privacy, confidentiality agreements between the bank, the network and the processors and also federal law.

As consumers have become comfortable with the use of ATM's and increasingly at the point of sale, they have asked for even greater convenience. Thus, they desire to interact with their banks and merchants from remote locations, like the home. Today, a consumer can perform electronic banking through either a telephone line or a personal computer. Initially, this was confined to transactions by a consumer with his own bank such as obtaining account balance information, transferring funds between accounts, finding out whether checks have been processed and cleared

through their account. All of these transactions remain within the customer's bank. Authentication is provided through the use of a password. This password is not the same as the PIN used in a debit transaction at an ATM or point of sale terminal. It is changeable by the customer at will. Moreover, these passwords are not encrypted and thus less secure. However, these transactions all take place within a single bank and thus are secure. As to privacy, all information is within a single bank and therefore there is no major issue.

Another service developed in the early 1980's and which has increasing interest from consumers is the ability for consumers to perform electronic banking which includes the payment of bills to merchants and others. In this particular circumstance, a customer establishes with his bank certain merchants on a file and regularly use either a telephone or a personal computer to direct their bank to make payments to these merchants. The bank either transfers funds through an automated clearing house or actually creates a check and mails it to a specific merchant. These transactions are within the banking system, providing assurance of payment. The funds will move only after the bank has authorized them. The authentication is provided by virtue of a password and the bank must make the authorization before it will make the payment. Security is provided by use of a changeable password. Again, privacy is provided by virtue of the fact that all instructions remain between the customer and the bank who will pay the merchant.

The past 20 years has seen the deployment of a substantial number of ATM's and Point of Sale terminals and a high level of acceptance of basic electronic services through financial institutions. It should be noted that today that there are more than 100,000 ATMs in the United States and it is projected that by the year 2000 there will be 200,000 ATMs. On the other hand, there are currently 20 million personal computers in the United States and that number is expected to expand to 50 million by the year 2000. The rapid increase of computer capability and steeply declining prices means people who never had access to computers will have and use them regularly. At the same time, there have been great advances in communications technology. Communications through fiber optics and other methods such as satellites and cellular transmission allow voice, data and graphics to be communicated through the same line.

These changes are exhilarating. They provide the ability to create a new level of convenience for the consumer in the conduct of his daily financial affairs. By the year 2000, most of those 50 million computers that are deployed will be capable of being used as though they were an ATM located in a person's home or in their office. Personal computers will allow them to conduct their everyday financial transactions efficiently.

We believe that these desires need to be satisfied. Electronic commerce is on the threshold of many new exciting services and we intend to provide them. Nevertheless, we are concerned about a number of very important issues. These issues strike at the very heart of system integrity. First, who controls the system and how is it monitored? This goes to the question of payment assurance and safety and soundness of the system. It also raises the question of who has jurisdiction over the system and whose laws will be applied. Concern is also raised over the ability to audit the system. This has implications for both tracking the money supply and for taxation. If you can't audit the system, then you can't determine the volume of money which flows through it. Moreover, an auditless system allows transactions which can't be tracked creating a major problem for taxing authorities.

Today, this Committee is inquiring about the development of commerce on the Internet. The Internet is an interconnection of computers in over 90 countries. There is no central authority which sets any standards or controls commerce over this communications facility. Entry to the system can come from many places and there is no central body through which all information must pass. The consequence is that there is no one body which can assure participants that the system has integrity.

How would a transaction take place? A consumer would use their computer to enter the Internet through a service that provides an entry point. Then the consumer would turn to a shopping page or if the specific merchant had an address on the Internet, the consumer would browse the offerings. To make a purchase, the consumer would fill out a form electronically and include a credit card number. The consumer must then wait for the goods to be shipped. But what happens if the goods never arrive? Today, the consumer has the protection of our credit card laws and rules of the card associations. In the world of electronic money these protections may not exist and there is the question of who has the authority to impose them. After all the person ordering the goods may be in the United States, but may be ordering from a

company in France, such as a case of wine, and the Internet connection may be through yet another country.
In these situations jurisdiction will have to be resolved and this is only the first level of issues.

In the context of Electronic commerce on the Internet, there are issues that we believe need to be examined and certain protections that must exist. First, we believe that the role of financial institutions in the payment systems mechanisms must remain paramount. Today there is a well developed body of appropriate regulations that protects the average person as to the safety and the soundness of their financial institution and provides assurances of the completion of the value exchange in our system. We think this should concern you as we move forward. Secondly, we believe it is critical that appropriate levels of authentication be provided in order to verify the transactions that are being requested and conducted are proper, appropriate and authentic. Thirdly, we believe that security is a critical factor. Electronic commerce up to this point has been appropriately controlled by parties who themselves are at risk and therefore have appropriate security controls in place. As we look at the Internet, its use and the global nature of this communications body, it is apparent that appropriate security methods must be properly developed and critical they be implemented. We also believe that privacy is a major issue. There are ever increasing concerns by citizenry that too much information about the individual is already available to too many parties. Issues such as privacy must be addressed in an appropriate fashion. If the consumer is to develop the confidence in the systems, he must not feel that these systems are intrusive on their personal life or expose their personal information without their control. In addition to these matters, the ability to audit, the ability to track the money supply and the authority to tax and enforce the collection of taxes mast be assured.

Today we stand on the edge of an electronic and communications frontier. We have a unique opportunity to provide needed services to our citizens for the conduct of their daily life. These services will be at a level of convenience and efficiency that has never before been possible. As you look at these issues we hope that you will focus your inquiry on these matters that concern us. Yet, we also hope that good judgment will guide you to avoid over regulation. We do not believe that high a level of regulation should be applied to areas which are in their infancy. We believe that you should be concerned about these basic issues. Protections in these areas will provide

the basis for achieving the confidence of the public in these systems as they develop while allowing them to direct their own course and develop in a natural way.

The Ease of Using Ecash

Overview

Ecash has been designed for ease of use. Consumers are given a simple "point-and-click" graphical user interface that is simpler to use than many bank ATMs. To demonstrate the ease of using ecash, various actual transactions involving two customers, Alice and Bob, are shown below.

Startup and Background Operation

Figure 1

Once Alice starts ecash, it runs on her PC in the background much like a memory monitor or clock program. While ecash is running, a small window is displayed that shows her the amount of ecash available to spend along with an optional toolbar that allows her to initiate various functions.

Withdrawing Ecash from the Bank

In order to use ecash to purchase goods or services, ecash must first be available on the payer's hard drive, just as cash is needed in a wallet to pay for goods or services in the physical world. Withdrawing ecash is as simple as withdrawing regular cash from an ATM. Alice simply enters the amount to be withdrawn from the bank and clicks the "OK" button. This amount of ecash is then transferred to her hard drive. The screen below shows the actual dialog box[1] used to withdraw ecash that appears when the bank icon has been clicked on the toolbar.

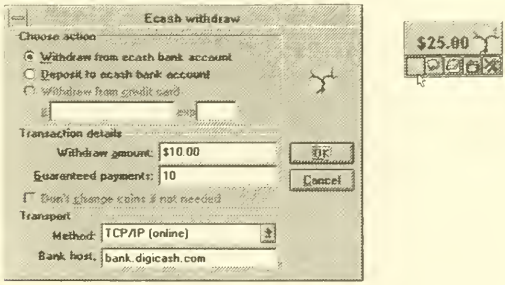


Figure 2

[1] Version 2.1 of the actual MS Windows ecash client is shown throughout.

Making a Payment

There are two ways to make a payment using ecash: responding to a payment request issued by someone else, or initiating a payment yourself.

Responding to a Payment Request

Bob may send a payment request to Alice who has asked to buy something. (Merchants' software will send such requests automatically.) For example, in the dialog box below, Alice is being asked to make a payment of $0.02 to start a tic-tac-toe game. If she wants to make the payment, the "Yes" button is clicked; similarly, clicking the "No" button will refuse the payment.

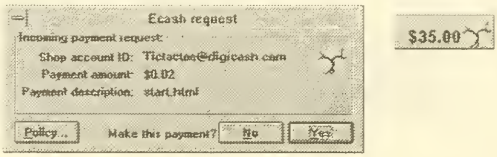


Figure 3

As an ease of use aid, Alice may also instruct her system to respond automatically to payment requests. When the policy button is clicked in the window above, the dialog box is extended downwards as shown in the window below, and she may set the policy under which payments are to be made automatically. This simplifies certain repetitive payments.

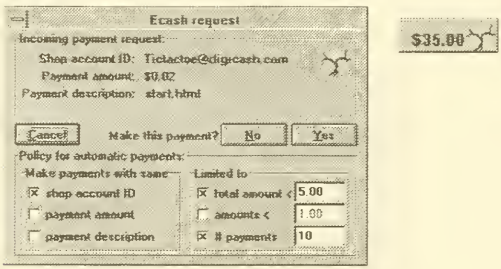


Figure 4

Initiating a Payment

To make an unsolicited payment directly, Alice brings up the payment dialog box from the toolbar and fills in the blanks, much like writing a check.

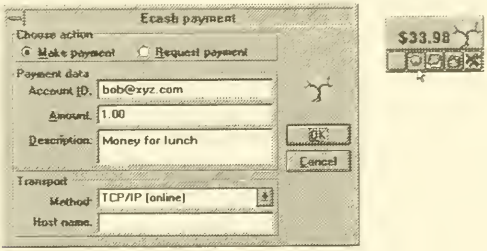


Figure 5

Receiving Ecash

When Alice pays Bob, he has the option of depositing ecash into the bank or retaining ecash on his hard drive for future use, as shown in the dialog box below.

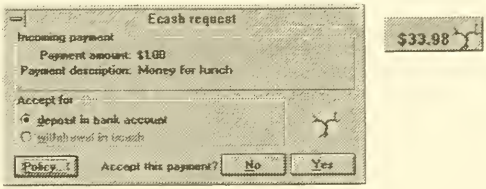


Figure 6

Just as Alice could set a policy for automatic response to payment requests, Bob can also set a simple policy for automatic handling of incoming payments, as shown below.

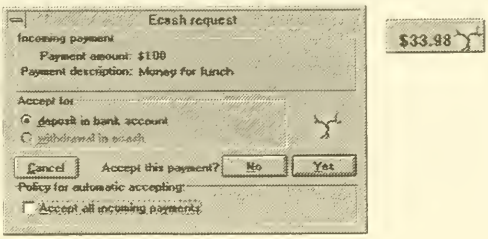


Figure 7

Depositing Ecash in the Bank

Ecash can, of course, be deposited in the bank. Again a simple dialog box is used. (Actually this is the same box as used in Figure 1 for withdrawals.)

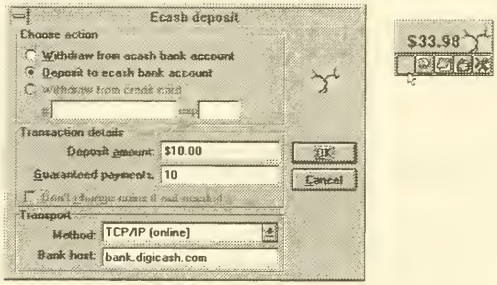


Figure 8

Receipts and Records

Ecash automatically tracks withdrawals, payments, receipts, and deposits, creating various electronic statements.

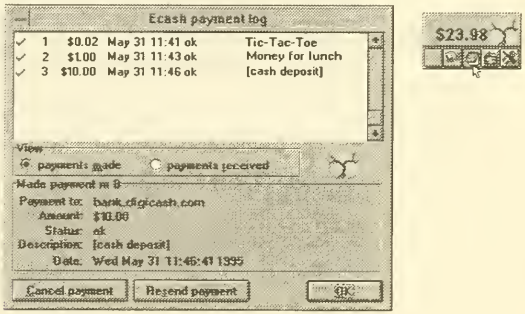


Figure 9

How Ecash Works Inside

Overview

Like banknotes, ecash can be withdrawn from and deposited to transaction demand deposit accounts. And like banknotes, one person can transfer possession of a given amount of ecash to another person. But unlike cash, during customer-to-customer transfers, banks will have an unobtrusive but essential role to play.

The following examples explain how a withdrawal works, followed by a payment to a retailer. Combining these two transactions, it is then illustrated how the system can be configured so that the customer perceives that ecash is paid from person to person without involving any accounts. Finally the withdrawal is explained in greater detail to illustrate the "blind signature" concept, which is the foundation of the privacy feature.

Simple Withdrawal of Ecash

Figure 10 shows the two participants in the withdrawal transaction: the bank and customer Alice. Also shown are the digital coins that have been withdrawn from Alice's account at the bank and are on their way to her PC. When they arrive, they will be stored along with the few coins left over on her hard disk.

Figure 10

Although of course no physical coins are involved in the actual system, the messages sent include strings of digits, each string corresponding to a different digital coin. Each coin has a denomination, or value, so that a portfolio of digital coins is managed automatically by Alice's ecash software. It decides which denominations to withdraw and which to use to make particular payments. (The ecash software contacts the bank in the rare event that change is needed before a next withdrawal, to let it restructure its portfolio of coin denominations.)

An Ecash Purchase

Now that Alice has some ecash on her hard drive, she can buy things from Bob's shop as shown in Figure 11.

Once Alice has agreed by clicking on the "payment request" dialog shown in Fig. 12 to pay a certain amount to Bob's shop, her ecash software chooses coins with the desired total value from the portfolio on her hard disk. Then it removes these coins from her disk and transmits them over the network to Bob's shop. When it receives the coins, Bob's software automatically sends them on to the bank and waits for acceptance before sending the electronic goods to Alice.

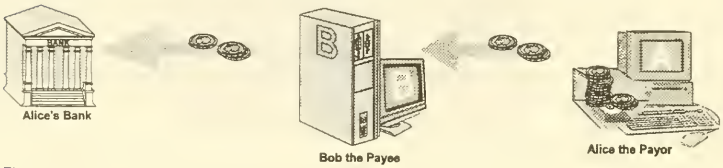


Figure 11

To assure that each coin is used only once, the bank uses the serial number of each coin to point to where it should be stored in the spent coin database it maintains. If the coin serial number is already stored at that position, the bank has detected someone trying to spend the coin more than once and informs Bob that it is worthless. If, as will be the usual case, no serial number has been recorded at that position, the bank stores it at that position and informs Bob that the coin is valid and the deposit is accepted.

Person-to-Person Cash

When a consumer receives a payment, the process could be the same. But some people may prefer that when they receive money, it be made available on their hard disk immediately, ready for spending—just like when someone hands them a five dollar bill. This user preference can be realized as depicted in Figure 12.

The only difference between this payment from Alice to another consumer, Cindy, and the one Alice paid to Bob's shop in Figure 11, is what happens after the bank accepts the cash. In Figure 12, Cindy has configured her software to request the bank to withdraw the ecash and send it to her PC as soon as the coins are accepted. (Actually Cindy's bank will check with Alice's bank to make sure that the coins deposited are good.) When Alice sends Cindy five dollars, that money is immediately available to spend from Cindy's PC.

Figure 12

How Privacy Is Protected

In the simple withdrawal of Figure 10, the bank created unique blank digital coins, validated them with its special digital stamp, and supplied them to Alice. This would normally allow the bank at least in principle to recognize the particular coins when they are later accepted in a payment. And this would tell the bank exactly which payments were made by Alice.

By using "blind signatures," however, a feature unique to ecash, the bank can be prevented from recognizing the coins as having come from a particular account. The idea is shown in Figure 13. Instead of the bank creating a blank coin, Alice's computer creates the coin itself at random. Then it hides the coin in a special digital envelope and sends it off to the bank. The bank withdraws the requested dollar from Alice's account and makes its special "worth-one-dollar" digital validating stamp on the outside of the envelope before returning it to Alice's computer.

Figure 13

When Alice's computer removes the envelope, it has obtained a coin of its own choice, validated by the bank's stamp. When she spends the coin, the bank must honor it and accept it as a valid payment because of the stamp. But because the bank is unable to recognize the coin, since it was hidden in the envelope when it was stamped, the bank cannot tell who made the payment. Thus the blind signature mechanism lets the validating signature be applied through the envelope. The signer can verify that it must have made the signature, but it cannot link it back to a particular object signed.

How It All Works with Numbers

The coins form a close analogy to the way it actually works in the ecash software. When Alice's computer creates a blank coin it chooses a random number. The bank's validating stamp on the coin is a public key digital signature formed by the bank with

the random coin number serving as the message signed. Checking the validity of a coin involves the verification of the digital signature using the bank's corresponding public key. The blinding operation is a special kind of encryption that can only be removed by the party who placed it there. It commutes with the public key digital signature process, and can thus be removed without disturbing the signature.

How Funds Flow

While for the consumer ecash is functionally equivalent to cash, to a bank its properties are somewhat different.

As can be seen in the top of Figure 14, the first step in each case is when value comes out of a customer's account. In an ATM transaction, the currency given to the consumer is a reduction in vault cash; in an ecash withdrawal, however, the value is moved within the bank and becomes an ecash liability that will be reversed when the ecash is presented for deposit.

The second step is the spending of the value. Here cash and ecash are very similar. In each case the merchant (or other party receiving it) has the option of accumulating or depositing it, as detailed later with reference to Fig 15.

When the merchant takes the final step and deposits the cash, it results in an increase in vault cash. A deposit of ecash reduces the ecash liability and increases deposit liability.

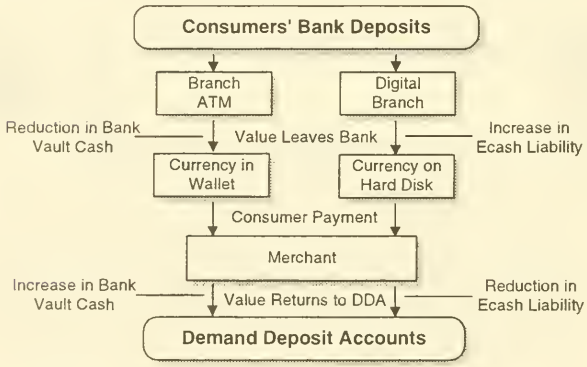
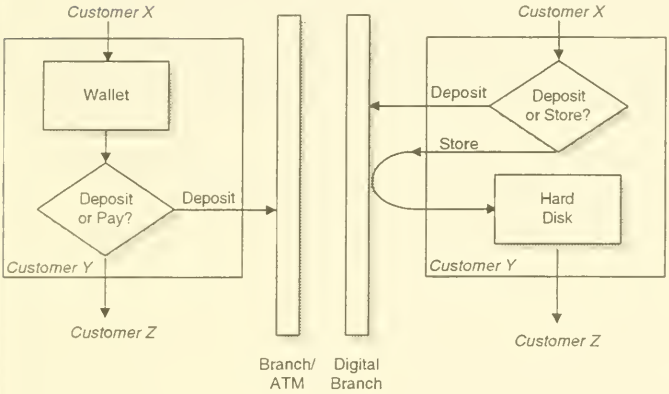


Figure 14

The chart below shows in more detail the difference in the actual transaction path for a cash payment and an ecash payment, particularly in the case where they are made from customer to customer. While the main difference is invisible to the consumer, it is necessary to protect the integrity of ecash.

- The left side of the chart shows a cash payment from Customer X, who may have originally withdrawn it, to Customer Y. The payment goes directly from X to Y's wallet, and at some later time Y has the option of either depositing the cash in the bank or using the cash to pay Customer Z. The process continues indefinitely until the cash is deposited.
- The right side of the chart shows an ecash payment from X to Y. Before the payment is accepted, Y verifies the validity of the ecash with the issuing bank, the main step which is not necessary with cash. Customer Y chooses at this time whether to store the ecash or deposit it immediately in the bank. If Y chooses to store the ecash, it may then later be used to pay Z, and so on.



ELECTRONIC PAYMENT SERVICES, INC.

DAVID M. VAN LEAR
Chairman and Chief Executive Officer
Electronic Payment Services, Inc.

David Van Lear is chairman and chief executive officer of Electronic Payment Services, Inc. (EPS), Wilmington, Delaware

Before his appointment as EPS chairman, Van Lear was a member of the EPS board of directors since its creation in December 1992, and chairman and chief executive officer of Banc One Corporation's Regional Affiliate Group from July 1992 to August 1993 From 1988 to 1992, he served as president and chief executive officer of Banc One Services Corporation, the technology services division of Banc One. He joined Banc One in August 1986 as senior vice president, responsible for product support.

Prior to joining Banc One, Van Lear held positions as senior executive vice president of American Savings & Loan in Los Angeles, and president of the Financial Services Group. From 1969 until 1984, he was with Norwest Corporation, serving as president of Norwest Information Services, Inc. from 1981 to 1984

Van Lear holds a B.S. in finance from San Diego State University He is also a graduate of the Amos Tuck Executive Program of Dartmouth College and the Colorado Graduate School of Banking.

Van Lear was selected as Chief Information Officer of the Year for 1991 and was featured in Information Week magazine.

ELECTRONIC PAYMENT SERVICES, INC.

Introduction

The formation of Electronic Payment Services, Inc. (EPS) has indelibly changed the face of the electronic funds transfer industry. Established in December 1992 as a joint venture between four major financial institution investors -- Banc One Corporation, CoreStates Financial Corp, KeyCorp and PNC Bank Corp. -- and with the addition of National City Corporation in 1995 -- the Company has become one of the leading electronic transaction processors in the United States, with 1 5 billion transactions annually. EPS is headquartered in Wilmington, Delaware and serves as the parent company for BUYPASS Corporation and MONEY ACCESS SERVICE INC A privately-held, for-profit company, EPS provides unsurpassed expertise in all components required to establish and operate automated teller machine (ATM) and point of sale (POS) networks and related systems The unique structure and vision of EPS allows it to make powerful investments in the research and development of new products and services, and positions the Company on the leading edge of industry capabilities Combined with extensive experience and commitment to customer satisfaction, EPS is unequaled in the electronic transaction services arena

ELECTRONIC PAYMENT SERVICES, INC.

Background

Since the formation of Electronic Payment Services, Inc (EPS), the dynamic business style of the Company has redefined the future of the electronic funds transfer (EFT) industry. The progressive structure of EPS, highlighted by the investors' common vision to operate delivery systems as a business -- not as a utility -- is driving the industry to abandon the non-profit model of operation. This has dramatically accelerated a trend towards consolidation The cultural and philosophical fit of the investors, a shared focus on customer service, and the consolidation of developmental resources, has enabled EPS to deliver an increasing array of innovative products and services to financial institutions, merchants and utilities. The ultimate goal of EPS is to be the premier provider of electronic transaction processing services. The key to EPS' success is its unique ability to carry the legacy of the founding organizations, and combine that depth and expertise with breakthrough vision and a continuing commitment to industry excellence. Highlighted among EPS' early milestones is the establishment of the Wilmington, Delaware headquarters; the creation of its 70,000 square-foot, state-of-the-art data center in Wilmington; the assembly of a talented, diverse management team; the addition of many major new customers; extensive growth in the Midwest, and the addition of a new investor. Through its subsidiaries, BUYPASS Corporation and MONEY ACCESS SERVICE INC., EPS offers high-quality, cost-effective transaction processing capabilities. The 900 associates of EPS share the belief that it's not just the products, but how those products are delivered, that differentiates EPS With the infrastructure now established, EPS will continue to make strategic investments to build for the future The Company will seek additional investors, identifying a select group of financial institutions that will further strengthen EPS' prominent position. Innovative new products will be introduced, headlined by the 1996 introduction of the stored value card using smart card technology. The smart card, which utilizes an embedded micro-chip to store value electronically, will be used in place of cash and coins for a multitude of retail purchases less than $20. An industry leader in smart card technology, EPS is the first company to receive Federal Reserve Board approval to provide processing for this product And as a member of the international consortium formed by Visa International, EPS will participate in the development of worldwide standards for the stored value card.

ELECTRONIC PAYMENT SERVICES, INC.

BUYPASS CORPORATION

Background

BUYPASS Corporation is a major third-party point of sale (POS) processor and the leading debit POS transaction acquirer in the United States, with access to most major automated teller machine (ATM) networks Headquartered in Atlanta, Georgia, BUYPASS pioneered industry-tailored technology for electronic data capture and funds settlement. It developed customized applications for petroleum, convenience store, supermarket, financial institution, hospitality, general retail and utility customers nationwide Services include host system-based POS terminal programming and management, settlement and adjustments, links to check authorization services, and electronic funds transfer (EFT) gateways. BUYPASS' groundbreaking achievements and experience over the past decade are unmatched It was the first third-party processor to pay merchants electronically, provide on-line debit POS transactions, access multiple networks, process ACH private label debit cards, and support a complete fleet management system. Through its Integrated Systems unit, BUYPASS has installed more electronic payment systems in supermarkets nationwide than any other processor BUYPASS offers an extensive array of integrated EFT/POS solutions for industry-standard platforms in the multi-lane retail and hospitality environments, including electronic cash register and property management systems With the formation of parent company Electronic Payment Services, Inc (EPS), consolidation and new business at BUYPASS in the early 1990s doubled the number of annual electronic authorization, draft capture and settlement transactions processed The Company operates 125,000 data capture terminals and processes 600 million transactions annually. BUYPASS' delivery of products emphasizes flexibility, integrity, continuous improvement, innovation and service This uniquely positions the Company to respond to the explosive growth in debit POS purchases Moving forward, the priorities of BUYPASS are to continue to develop market-specific technology applications, expand transaction services to include a broader range of data movement to improve customer access to business information; maintain the leadership position in integrated EFT/POS solutions for new and existing high-end systems through strategic cooperation with various hardware manufacturers; identify and implement efficiencies to support highly competitive pricing; expand current services to include additional data transmission applications such as electronic benefits transfer, and increase the delivery of host-to-host gateway services

ELECTRONIC PAYMENT SERVICES, INC.

MONEY ACCESS SERVICE INC.

Background

MONEY ACCESS SERVICE INC. (MAS), headquartered in Wilmington, Delaware, is the operator of the MAC® network. A super-regional electronic funds transfer (EFT) network, the Company leads the United States in the delivery of branded financial, retail and information transaction services as the largest processor of switch transactions. Currently, the network is comprised of 1,700 financial institution members, 18,200 automated teller machines (ATMs), 150,000 point of sale (POS) terminals, and 32 million cardholders in 34 states. Processing 900 million switch transactions annually, MAS is three times larger than the nearest competitor. With the formation of parent company Electronic Payment Services, Inc. (EPS), the MAC network merged with regional networks Green Machine, OWL and Trinet, and incorporated Banc One's proprietary Jubilee network under the MAC brand. As the integration of these networks continues in 1995, the strongest capabilities of each network will be combined to create the "best of the best" under the MAC brand. The next step will be the consolidation of the products and processing platforms of each network. The synergies created by the merger will allow the MAC network to invest substantially in the research and development of innovative new products and services. MAS currently provides a multitude of enhanced cardholder services, including MAC Check®, MAC Info® and MAC Phone®. This new generation of self-service banking offers an array of capabilities including check cashing to the penny, split deposits, bill payment and loan calculations. MAS provides a complete value-added package to customers, including marketing and consultative services, ongoing training, regional and annual conferences, and the ability to customize products and services. The direction of the MAC network is based on more than depth of expertise, it is customer- and market-driven. The MAC Advisory Council, consisting of a representative group of financial institutions, meets on a quarterly basis to discuss network members' needs and to provide a forum for input. As the MAC network moves into the future, members will see the implementation of advanced multi-site data center capabilities, featuring the most robust disaster recovery system in the United States. Network members will also benefit from leading edge product development and technology, continued emphasis on the POS business and home-based banking services, consistent investment in the MAC brand, and a renewed focus on exceeding customer expectations.

Reprinted from

AMERICAN BANKER

The Daily Financial Services Newspaper

Thursday, April 6, 1995

Network Pushes Ahead With Smart Card Trial

Trial Run For a New Payment System

Jennifer Mariner of Electronic Payment Services Inc. uses a smart card to buy postage stamps, demonstrating "electronic purse" technology that the company expects to be deploying in Delaware by early next year.

EPS Delaware Smart Card Test
Pictured above

Location	Two zip-code areas in Wilmington
Cards	Distribution through 600 bank branches
Merchants	150
Rollout	First quarter 1996
EPS owners	•CoreStates Financial •National City •PNC Bank •Keycorp •Banc One
Banks	Partners for pilot are undisclosed

Visa U.S.A. Olympic Smart Card Project

Location	Atlanta
Cards	1 million (disposable and rechargeable)
Merchants	5,000
Rollout	Summer 1996
Banks	•First Union •NationsBank •Wachovia

By VALERIE BLOCK

Electronic Payment Services Inc. is forging ahead with its smart card trial in Delaware, undaunted by the fact that other tests — like Visa U.S.A.'s plan for the Atlanta Olympics next year — will be far bigger.

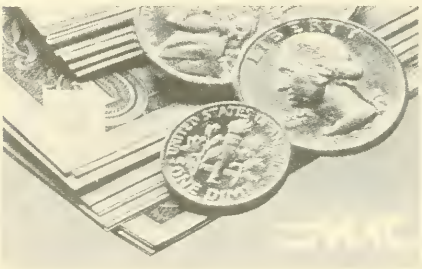
Wilmington-based EPS, best known for operating the MAC automated teller machine network, began an in-house pilot test in February that will act as a model for the rollout to two New Castle County zip codes in early 1996.

"Before we roll out, we want a thorough understanding of consumer needs and perspectives" relating to the new chip technology, John F. Beahn, chief marketing officer, said recently in the company cafeteria while eating a lunch purchased with one of the stored-value cards.

The cards, which have been distributed to the 400 employees at EPS' headquarters, function at nine vending machines, six cash-to-card loaders, three stamp machines, three public telephones, and the cafeteria.

Although the company has been running a 4,000-employee test at CoreStates Plaza in Philadelphia since 1991, the newer program includes updated technology that will mirror the Delaware rollout, said Mr. Beahn.

Upon entering the main building of the EPS compound, on 26 green acres just outside downtown Wilmington, employees can load value onto their cards at the cash-to-card dispensers in the electronic banking center.



THE CARD USES a microcomputer chip from France's Gemplus to track cash-equivalent debits and credits.

The microcomputer chips in the cards, manufactured by Gemplus of France, track the cash-equivalent debits and credits. The initial cards were free; an extra card costs $1.

Karen Strauss, technology training manager, loads a weekly cash allotment onto her card and carries it in her employee identification pouch, which clips onto her clothing.

"We do a lot of running around here," she said while standing in line at the cafeteria. Now "I don't have to go upstairs to get money" for lunch, she said. "It's right here."

While employees are learning about the convenience of stored value, EPS is ironing out the kinks for the larger project, previously scheduled to begin in October but delayed until early next year, said David M. Van Lear, chairman and chief executive officer.

In that trial, 50,000 cards issued by a still undisclosed group of participating banks will be linked to consumers' checking accounts. Users will be able to add value through automated teller machines and to purchase goods from about 150 merchants.

In a recent presentation, EPS executive Bernard David listed banks heavily represented in New Castle County: Bank of Delaware, Beneficial National Bank, Delaware Trust Co., Mellon Bank, and Wilmington Trust Co.

Until only a month ago, EPS' program was regarded as the most ambitious stored-value pilot planned for the United States. But Visa's 1996 Olympics program, led by First Union Corp., NationsBank Corp., and Wachovia Corp., "has already overshadowed" EPS, said Liam Carmody, president of Carmody & Bloom, Woodcliff Lake, N.J.

"The Atlanta pilot will be very visible; the Olympics get a lot of attention," the consultant said.

Visa said at least one million disposable and rechargeable cards will be distributed during the Olympics, for use at 5,000 participating merchants.

Mr. Van Lear, 53, chairman of EPS for the past year and a half, said the launch in Atlanta would not affect the plans of EPS, a joint venture of Banc One Corp., CoreStates Financial Corp., Keycorp, National City Corp., and PNC Bank Corp.

The technology to be used in the Olympics effort "is not the long-term solution," said Mr. Van Lear, a former Banc One executive.

Diane Wetherington, senior vice president of chip card

David Graham

FOUR HUNDRED Electronic Payment Services employees are using an experimental cash card at the headquarters cafeteria and elsewhere in preparation for a 50,000-user pilot test.

marketing for MasterCard International, said as much last week when MasterCard said it would launch its own stored-value pilot in Australia in the fourth quarter.

Visa's pilot "is an event-related situation," Ms. Wetherington said. "What's more interesting for us is an ongoing relationship with the cardholder, as opposed to something cardholders can use for only four weeks."

First Union said it is planning an open system, scheduled to kick off in Atlanta this September with 300,000 chip ATM cards issued to residents. But some industry observers doubted First Union could meet those goals.

Mr. Carmody pointed out that various competitive approaches "can come together," with the initiatives eventually building off each other. Mr. Van Lear said EPS will be on the leading edge, having "influence over the marketplace." He added that international standards must be set so merchants the world over will be able to use the same equipment to accept the cards.

To that end, EPS is involved with the International Standards Organization, the American National Standards Institute, and Visa's international stored-value working group.

EPS has yet to join the Smart Card Forum, a multi-industry group promoting testing and standardization, though there have been rumors that EPS is opening up to the possibility. It was concerned about sharing results of its advanced work with competitors.

The EPS trial will "prove a lot of stuff" about what you can do with the card, said Mr. Van Lear. "We'll compete on the application side, getting banks to issue our cards" rather than those of competitors, he said. The banks will "belong to our network."

Mr. Van Lear said the delay until 1996 was partly to ensure that the technology will not be quickly supplanted by something more advanced.

The Delaware rollout will emphasize vending machines, transportation, and retail points of sale. Some activity may eat into debit card volume, Mr. Van Lear said.

Other stored-value programs around the world, like the Danmont program in Denmark, focus on small-change purchases such as newspapers, phone calls, and parking meters, and are said not to cannibalize debit or credit cards.

"We're going for ubiquity," said Mr. Van Lear. "We don't want multiple cards, we want multiple applications [on one card]. We're going for the highest value."

Mr. Van Lear foresees considerable interest in vending machine areas in supermarkets, selling everything from stockings to batteries, six-packs of soda to suntan lotion.

Danyl Corp., a Schlumberger division headquartered in Moorestown, N.J., is manufacturing the smart card readers for the pilot. Peter J. Truscello, Danyl's president, agrees there is a big market for unattended vending machines.

Mr. Van Lear said merchants will embrace the technology,

which would help reduce labor costs by shrinking lines in supermarkets.

But Dan Shanahan, vice president, point of sale for Tops Friendly Markets in Buffalo, said, "People like variety. We have 32 [shelf] feet of stockings — that's very wide. You'd need a big vending machine."

Vending machines can work for items like a pack of gum, he said, but for many things "people love to shop."

Mr. Shanahan said the stored-value concept would be most useful at express registers where people insist on using cash.

Still, Mr. Van Lear said, EPS got "very positive reaction from merchants" in Delaware, who see the new technology as cheaper than cash. Gas stations, toll collections, and fast food are other areas where the system should be popular, Mr. Van Lear said.

As the technology catches on, issues regarding ownership of money stored in the cards but never spent — sometimes called float or breakage — will prove complicated.

Mr. Shanahan said banks shouldn't control electronic money once it's out the door. But Mr. Van Lear said money stored on the card hasn't exactly left the bank until its spent.

"It's a transaction waiting to occur," he said, adding that the settlement questions will not be answered overnight. □

The New York Times

Business Day TUESDAY, SEPTEMBER 6, 1994

An End to the 'Nightmare' of Cash?

by SAUL HANSELL

The relentless march of technology into the smallest details of everyday life may be reaching the final frontier: the advent of the electronic penny.

Banks, credit card companies and even the governments of some countries are racing to introduce "electronic purses," wallet-size cards embedded with rechargeable microchips that store sums of money for people to use instead of cash for everything from buying fast food to paying highway tolls.

With 80 percent of the 360 billion transactions in the United States each year paid for with cash, and 90 percent of that 80 percent involving amounts of less than $20, the theoretical appeal of the electronic purse, or stored-value card, seems clear.

Cash Is 'Inconvenient'

"What consumers want is convenience, and if you look at cash, it's really quite inconvenient," said Donald J. Gleason, president of the Smart Card Enterprise unit of Electronic Payment Services, known as EPS, which runs the MAC cash machine network. "And for merchants, cash is a nightmare. It is expensive to handle, count and deposit, and they have slippage, which is their way of saying theft."

EPS has the most advanced plans for the introduction of a stored-value card in the United States, starting in Delaware next year. The company, which is based in Wilmington, Del., and owned by half a dozen large Northeastern and Midwestern banks, hopes to attract other banks and automated teller machine, or ATM, networks around the country to join in and build a nationwide electronic purse system.

Both Visa International and Mastercard International are also working on ventures to take the so-called smart card, introduced a decade ago, into the bold new world of information technology.

A pocket card that carries a microchip is, in effect, a small computer—a more advanced version of the cards with magnetic stripes used by people in New York and Washington to pay for subway fares.

In recent years, some telephone companies in other countries have marketed smart cards that were charged with a set number of calls. The State of Ohio is developing a smart card system for the electronic delivery of welfare benefits. Other uses under discussion range from electronic drivers licenses to the storage of medical records.

"Think of it as your PC, which you bought for office applications, then added other software later," Ronald A. Braco, senior vice president for electronic banking at Chemical Bank, said of the smart card, which Chemical is testing in its employee cafeteria. "We can download other applications to the card at an ATM or over the telephone."

But the first application that experts say will widely deploy smart cards will be the electronic purse.

After it is loaded with money, at an ATM or through the use of an inexpensive special telephone, the electronic purse can be used to pay for, say, candy in a vending machine equipped with a card reader.

The vending machine need only verify that a card is authentic and there is enough money available for a chocolate bar. In one second, the value of the purchase is deducted from the balance on the card and added to an electronic cash box in the vending machine. The remaining balance on the card is displayed by the vending machine or can be checked at an ATM or with a balance-reading device. Such a system would virtually eliminate fumbling for change or small bills in a busy store or rush-hour toll booth, and waiting for a credit card purchase to be approved.

"What consumers want is convenience, and if you look at cash, it's really quite inconvenient," said Donald J. Gleason, president of the Smart Card Enterprise unit of Electronic Payment Services.

And when the balance on an electronic purse is depleted, the purse can be recharged with more money. As for the vendor, the candy machine's receipts can be collected periodically in person—or, more likely, by telephone—and transferred to a bank account.

The cost and timing are the keys. While the technology has been available for a decade, the cards have been relatively expensive, from $5 to $10. Now the cards cost $1, and special telephones that consumers could install at home to recharge the cards are projected to cost as little as $50. A simple card reader would cost a merchant less than $200.

What is holding the cards back? Long-range planners in the

banking industry see the weaning of small businesses and consumers from cash as the last step to closing many expensive branches and conducting virtually all business by telephone, through cash machines and perhaps home computers.

"Banks estimate that 4 percent of the value of cash that is deposited gets eaten up in handling costs" said Michael C. Nash, a senior vice president with Visa International.

Despite the advantages of electronic purses, some analysts say the banks face a struggle convincing consumers that they need another type of card.

One reason is that more people are using credit cards for more small purchases than in the past. That is in part because credit card terminals are increasingly capable of handling transactions faster and because of the proliferation of cards that offer bonuses like frequent-flier miles for purchases. And in many areas, consumers have just begun to warm to the debit card, which works like a check, making purchases by deducting money from a customer's bank account.

Another reason is that in many electronic purse plans, a lost card is the same as lost or stolen cash: it's gone.

Promoters like Mr. Gleason counter that customers can load up their card with only as much money as they feel comfortable carrying, refilling them every night by telephone.

"Could anything be safer than loading value onto your card in the convenience of your home or office?" he asked.

Ambition Abroad

Matters are far more advanced abroad. Banking groups in Denmark, Portugal, Singapore and other countries are sponsoring electronic alternative to small change. And two of Britain's largest banks, National Westminster Bank P.L.C. and Midland Bank P.L.C., along with British Telecommunications P.L.C., are about to introduce an especially ambitious system known as Mondex, which they hope to establish as a worldwide system of cards that can be loaded with five currencies at one time.

An elaborate trial of Mondex, involving 40,000 card holders and 1,000 merchants in Swindon, England, is scheduled to start next year; its debut is expected in 1996.

The most extensive deployment of the technology so far has come in Denmark, where a consortium of banks and telephone companies, known as Danmont, has issued more than 150,000 stored-value cards, aimed at very small transactions like those at parking meters and soda machines. One of the most popular applications has been in laundromats, which have found that the cards reduce theft and vandalism and increase sales.

"Before, people would only have enough coins for two machines, color and white," said Henning N. Jensen, managing director of Danmont. "Now they split the colors into hot and cold."

Danmont makes money by earning interest on the money it holds on the cards, called the float, and by charging vending machine owners who use the system about 3 cents a transaction. Bankers in the United States said merchants would be willing to pay more, perhaps 10 to 15 cents, for the privilege of handling less cash. And they hope to charge consumers a monthly or annual fee to use the card.

Home Shopping Applications

Some American bankers say the security of smart cards will make them most useful for payments on electronic home shopping and video services.

"As more and more people do business on the Internet, we have to look for how you pay for things," said Catherine Allen, a vice president in Citibank's technology office and the head of the Smart Card Forum, an industry group. "The smart card allows me to identify myself securely."

Citibank has introduced a telephone with a computer screen and a smart card reader for identification in its home banking service. The bank expects the phone to eventually be used to add money to electronic purse cards.

But Mondex has still another wrinkle: privacy.

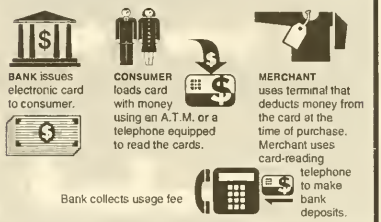
Unlike most other electronic purse systems, Mondex, like cash, is anonymous. The banks that issued Mondex cards will not be able to keep track of who gets the payments. Indeed it is the only system in which two card holders can transfer money to each other.

While many bankers are concerned that the system will be left open to fraud and abuse, Mondex executives say anonymity and flexibility are vital to acceptance.

"If you want to have a product that replaces cash, you have to do everything that cash does, only better," Mondex's senior executive, Michael Keegan said. "You can give money to your brother who gives it to the chap that sells newspapers, who gives it to charity, who puts it in the bank, which has no idea where it's been. That's what money is."

How Electronic Purses Work

Electronic purses work like electronic cash. Consumers transfer money from their bank accounts on to cards embedded with computer chips and then carry them around to use like cash. Using them is faster than using a credit or a debit card, but there are risks.



Pros and Cons of Electronic Purses

ADVANTAGES	DISADVANTAGES
FOR CUSTOMERS	
■ Transactions in a second; no need to wait for change. ■ Eliminates the need for exact change at vending machines and pay phones. ■ Card can be recharged at home by a special telephone.	■ Money on card does not earn interest. ■ Unlike credit cards, no replacement if lost or stolen. ■ Unlike cash, bank may charge fee for use of card. ■ Unlike checks, no paper trail.
FOR MERCHANTS	
■ Eliminates the cost of handling cash and the risk of theft. ■ Transaction fee is less than for credit cards or debit cards. ■ Devices that read the cards don't need to be plugged into a phone line.	■ New equipment (card reader) required. ■ Transaction fee
FOR BANKS	
■ Fees from merchants and consumers. ■ Can invest the money carried on cards until it is spent. ■ Reduced use of cash means reduced need for branches.	■ Expense of setting up system and modifying automated teller machines. ■ Risk of fraud. ■ May encourage customers to switch from credit cards, which are more profitable.

N.Y. Times News Service

THE FUTURE

Cover Story

In his pinstriped suit and wire-rimmed glasses, Timothy L. Jones looks every bit the traditional British banker. Sure enough, he has spent a dozen years at National Westminster Bank PLC. But ask Jones what he is doing now, and he responds with an intensity worthy of a Silicon Valley entrepreneur. Leaning across a table, he waxes eloquent about his new enterprise, Mondex, and the future of the product he's selling: a new kind of electronic money.

Mondex, which was launched by NatWest, is not alone: A raft of companies are developing their own forms of electronic money, known as E-cash. E-cash is money that moves along multiple channels largely outside the established network of banks, checks, and paper currency overseen by the Federal Reserve. These channels enable consumers and businesses to send money to each other more cheaply, conveniently, and quickly than through the banking system.

Some of the E-cash players are faceless, dubious outfits that exist in cyberspace and can be traced only to a post-office box—in the physical world. But there are plenty of others, ranging from techno-savvy startups with names such as DigiCash and CyberCash, to corporate icons including Microsoft, Xerox, and Visa. Citicorp is even developing what it calls the Electronic Monetary System, an entire infrastructure for using electronic money to be issued by Citi and other banks.

These companies are part of a mass experiment that could transform the way we think about money. In the process, it could change consumers' financial lives and shake the foundations of global financial systems and even governments.

Digital money is the ultimate—and inevitable—medium of exchange for an increasingly wired world. With E-cash, you'll no longer need to carry a wad of bills in your pocket or fumble for exact change. Instead, you might carry a credit-card-size piece of plastic with an embedded microchip that you will "load" up with E-money you buy with traditional currency. Or, you might store your digital coins and dollars—downloaded over phone lines from your bank or other issuer of E-money—on your PC or in an electronic "wallet," a palm-size device used to store and transmit E-money.

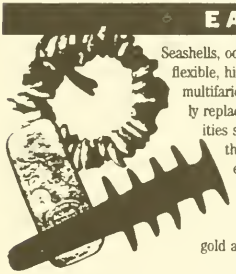
This digital money will let you shop online, zapping money to a merchant over the Internet, or perhaps paying for a movie on demand over an interactive-TV network. It also has the potential to replace cash and checks for everyday purchases—in stores, restaurants, or taxis that accept E-cash. Businesses could also keep a stash of E-cash on hand for buying office supplies, or use it to transact directly with each other instead of going through banks and electronic funds transfers.

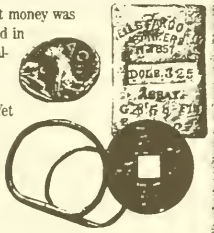
THE START OF A REVOLUTION. In many ways, E-cash, which can be backed by any currency or other asset, represents the biggest revolution in currency since gold replaced cowrie shells. Its diversity and pluralism is perfectly suited to the anarchic culture of the Internet and the evolving web of networks known as the Information Superhighway. "Electronic commerce will literally change the way business is done worldwide," says James G. Cosgrove, vice-president and general manager for business multimedia services at AT&T. "We're about to see another revolution similar to the Industrial Revolution." Adds Richard K. Crone, senior manager in the financial-services group at KPMG Peat Marwick: "We're in the beginning stages of the cash-replacement cycle."

But the advent of E-cash raises all sorts of questions, most of which remain unanswered: Who should be allowed to issue E-cash, and who will regulate those issuers? How will taxes be applied in cyberspace, which transcends physical boundaries? Who will set the standards? How do you ensure that payments made over the Net will be secure? How will consumers be protected?

EARLY MONEY

Seashells, odd rough-hewn coins—the first money was flexible, highly distinctive, and exchanged in multifarious ways. Objects were gradually replaced by standardized commodities such as gold and silver, and these in turn by paper money. Yet even early currency was at first issued by private banks, local governments, and others—usually backed by gold and silver. Diversity abounded.





OF MONEY

E-cash could transform the world's financial life

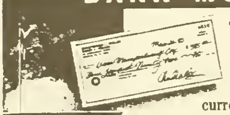
How will regulators police money laundering and counterfeiting on private networks?

While regulators wrestle with these questions, technology is remaking the monetary system. That's what Microsoft CEO William H. Gates III had in mind when he bid for personal-finance software maker Intuit Inc. He saw programs such as Intuit's as the gateway that would draw millions of consumers onto his online network where they could pay bills, get financial advice, or shop, perhaps paying him for access. But the Justice Dept. worried about Microsoft's reach, and he abandoned the deal on May 20.

Tough break, but it will hardly slow Gates down. Microsoft is working with Visa on a system for securing credit-card transactions over the Net. But that's just one piece of a much bigger problem Microsoft is trying to solve. Gates has dozens of programmers busy devising a sweeping system, Microsoft Network, to help people do business safely in cyberspace—or more specifically, in Microsoft's own network and interactive-TV systems—using a range of payment options. Microsoft won't reveal much about its E-cash plans, but, says Nathan P. Myhrvold, Microsoft's top advanced-technology expert, "we're very interested in the area."

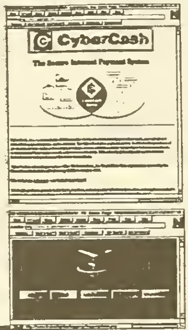
They should be. The stakes are enormous. Seamus McMahon, a vice-president at Booz, Allen & Hamilton, sees as

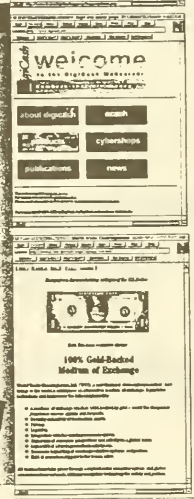
BANK MONEY



The current money system is largely monolithic. Nearly all major countries have a single system of national currencies and bank checks. Most have elaborate infrastructures built around commercial banks and a central governing body such as the Federal Reserve Board. That entity is usually the only facility allowed to issue money. Perhaps because of their monopoly structures, money systems tend to resist change and innovation. Traders can move millions of dollars around the globe at the touch of a button. But the small check-based transactions of consumers can take days to clear. And chartered airplanes physically transport billions of checks around the country every workday.

E-CASH





E-cash may be technologically light-years ahead of early money. But in many ways, it is closer to seashells than greenbacks. E-cash is digital money that moves through a multiplicity of networks instead of the current bank system. It comes in lots of guises, is created by lots of individual parties, and is backed by anything constituents demand as an accepted medium of exchange: gold, dollars, yen, whatever. It is the ultimate, and inevitable, currency for the wired world. Competition is intense, producing rapid innovations. Using money downloaded to your PC or a palm-size electronic "wallet," you'll be able to zap money to merchants on the Net—or buy a newspaper faster than you can grab a greenback. If you're a business owner, you can bypass banks and move E-cash directly to customers and suppliers. The advantages: convenience, speed, cost savings. The technology is complex, but to the user, E-cash is as easy as pushing a button.

EARLY MONEY (CLOCKWISE FROM FAR LEFT) PHOTOGRAPHS BY FPG, GABE PALMER/PALMER/KANE, INC./STOCK MARKET, TED MAHIEU/STOCK MARKET, FPG; PAMELA DEWEY/NATIONAL MUSEUM OF THE AMERICAN INDIAN, FPG, FEDERAL RESERVE BUILDING, PHOTOGRAPH BY JEFF SHELMAN/IMAGE BANK

much as 20% of total household expenditures taking place on the Internet just 10 years from now. If any operation, whether Citicorp or a startup such as Mondex, gained control of a new medium for even part of those exchanges, it would have the opportunity to charge royalties or fees for its use and earn interest on the E-money sitting in its accounts. Even a tiny charge, when applied to millions of transactions, would be highly lucrative.

E-cash could also create a competitive free-for-all. Because the Internet knows no boundaries, a company offering E-money can gain direct access to millions of consumers and businesses—no matter what state or country they are in. "The retail banking market will collapse and give way to global competition," says Eric Hughes, president of Open Financial Networks, a Berkeley (Calif.) consulting firm. "Those [regional] separations don't work on the Internet."

WINNING CONSUMERS' TRUST. Governments' and central banks' control of money flows has already been loosened, as shown by recent currency and market crises in Mexico and elsewhere. But with the growth of E-cash, money could flow in and out of countries at lightning speed without being traced, weakening governments' ability to monitor and tax. "Over the long haul, this is going to lead to the separation of economy and state," declares Bill A. Frezza, president of Wireless Computing Associates and co-founder of the advocacy group DigitaLiberty.

The growth of E-money could also be bad news for banks. If other companies successfully offer their own brand of digital cash, they could bypass banks as primary providers of consumer financial services. The companies, not the banks, might be consumers' first contact when they wanted to obtain some digital money. "Banking is essential to the modern economy, but banks are not," says J. Richard Fredericks, senior managing director at Montgomery Securities.

Commercial banks are, of course, entrusted with the creation of money through the fractional reserve system. They can lend more than they have on deposit, and they are the only companies authorized to do so. If each unit of E-cash had to be backed by a corresponding unit of traditional currency, that would mean that lending out E-cash wouldn't create new money. But if nonbank money suppliers started backing just a fraction of their digital cash with traditional money—just as commercial banks today keep on hand only a fraction of the deposits on their books—nonbanks, which are largely unregulated, could create money just as commercial banks do now.

This could be bad news for banks. What if phone companies offered their own brand of E-money?

Bankers must move fast to keep up. Ronald A. Braco, head of electronic banking at Chemical Bank, estimates that banks have less than five years to come up with viable E-money products before other players carve out the biggest chunks of the market for themselves. "No question, it's for real," says Richard M. Rosenberg, chairman and CEO of BankAmerica Corp. In a couple of years, "it will take off fairly dramatically." The issues now: winning consumers' trust and getting them to change their buying habits.

The first step in that direction could be to get consumers used to using credit cards for purchases on the Internet. Once that happens, the thinking goes, they may be willing to start using E-cash systems.

One of the first purveyors of a Net credit-card system is First Virtual Holdings, run by onetime celebrity manager Lee Stein. Stein has launched a relatively simple system using E-mail that lets consumers use credit cards on the Internet without fear that their account numbers will be misappropri-

The New World Of E-Cash

THE GOOD

- E-cash may be more convenient and flexible than traditional money. It can be used by consumers and businesses, and for everything from buying wares on the Internet to lending a pal five bucks.
- Banks that issue E-cash could find it much cheaper than handling checks and the paper records that accompany traditional money.
- Consumers doing business on the Internet will find some forms of electronic money afford much greater privacy than using ordinary credit cards.

THE BAD

- Uncontrolled growth of E-cash systems could undermine bank- and government-controlled money systems, giving rise to a confusing and inefficient Babel of competing systems.
- E-cash may be less secure than bank money: Money stored on a PC could be lost forever if the system crashes.
- E-cash could foster a have and have-not society: Those with PCs would have ready access to the stuff, while those without, many of them low-income consumers, would not.

AND THE UGLY

- Money laundering and tax evasion could proliferate in stateless E-money systems as criminals use untraceable cyberdollars to hide assets offshore.
- Counterfeiters could create their own personal mints of E-cash that would be indistinguishable from real money.
- If computer hackers or other criminals were to break into E-cash systems, they could instantaneously filch the electronic wealth of thousands or even millions of innocent consumers.

DATA: BUSINESS WEEK

ated. The card numbers are stored away on a protected computer system and never pass over the network. Instead, consumers register with First Virtual by phone and receive I. D. numbers in exchange for their card numbers. When they want to buy something electronically, they simply supply their I. D. number to the merchant.

First Virtual, which became the first secure payment system on the Net when it handled its first transaction last October, is growing fast. Stein won't disclose activity levels, but he says volumes are increasing by 16% a week. "If you make it simple and safe, people will use it," he says. First Virtual has enlisted such merchants as Apple Computer, Reuters, and National Public Radio—which sells transcripts of programs.

Most electronic extensions of the credit-card system, though, are built around encryption—scrambling card numbers so they can pass safely on electronic networks. For example, CyberCash Inc., a Reston (Va.) startup, is cutting its teeth on a deal with Wells Fargo & Co. for encrypted credit-card transactions over the Internet.

Visa and MasterCard, not surprisingly, are also working to make credit cards usable on the I-way. Visa is, among other things, developing with Microsoft a system using encryption technology that they hope will become an industry model. "We want to be sure that the industry as a whole has certain standards," says Carl F. Pascarella, president and CEO of Visa USA. Meanwhile, MasterCard has teamed with Netscape Inc., a maker of security and browsing software for the Internet, to pursue a similar goal.

WILTSHIRE EXPERIMENT. Credit-card-based systems have the advantage of seeming familiar to consumers. But the card systems don't do everything cash can: They're not anonymous, they do not work person-to-person, and they have credit limits. They're also not suited for the grassroots economy the Internet makes possible, where any outfit or individual can sell its wares, whether a newsletter or a stock tip.

That's where E-cash comes in. But E-cash needs to be just as secure as credit cards for people to use it. David Chaum, CEO of pioneer DigiCash in Amsterdam, has done the most to solve this problem. He has devised a clever system that uses so-called public-key cryptography that, like encryption, makes it possible to send sensitive information over the Net. But Chaum's big breakthrough was "blinding" technology, which lets the issuing bank certify an electronic note without tracing whom it was issued to. The result: Your E-cash, unlike an encrypted credit-card transaction, is as anonymous as paper cash.

Chaum has yet to announce firm deals with companies to issue his E-money. But in a pilot, some 5,000 consumers are part of a DigiCash marketplace, using the equivalent of $1 million in E-money to do business with 50 companies, from Encyclopaedia Britannica Inc. to Ricky's Junk Shop. Chaum's technology is also at the heart of CAFE, a European Commission-sponsored project to develop an electronic wallet for pan-European use.

CAFE's setup is similar to Jones's Mondex system. "Imagine it's the same as physical money, and you won't be far off," says Jones. Mondex money will be created initially by NatWest and a partner, Midland Bank PLC, which will then "sell" it to customers. The E-money is loaded onto credit-card-size "smart" cards with embedded microchips. The cards can be used in point-of-sale terminals or fit into electronic wallets that can transmit money to merchants or—just as with traditional cash but not with credit cards—to other consumers. Mondex money is still in pilot form, but the company has signed up 40,000 consumers and over 1,000 retailers in the Wiltshire town of Swindon to test Mondex money beginning in July.

CyberCash, too, is experimenting with E-cash in addition to its credit-card-based system. In the E-cash system, consumers will set up E-money accounts at their banks. Then, using proprietary software provided free of charge by CyberCash, they can go about their business on the Net. At the end of the day, CyberCash will clear all the E-money transactions and convert E-cash balances back to dollars.

No matter who develops the best E-cash, consumers and businesses alike stand to reap sizable benefits. No longer will consumers have to wait for change or scurry to automated teller machines for cash—out of sight, they hope, of the nearest mugger. E-cash will let businesses carry out transactions around the world without transferring bank funds—and they will be better able to reach a large population of technologically savvy, often affluent consumers.

Moreover, because E-money is basically software, it can be programmed to do things that paper money could never do. Microsoft's Myhrvold explains that electronic money could be

ROBERT BURROUGHS

CREDIT CARDS IN CYBERSPACE

"If you make it simple...people will use it"

— LEE STEIN, CEO, First Virtual Holdings

earmarked for special purposes, with conditions on where it can be spent. For example, a business could have an electronic version of petty cash to be used for supplies at an Office Depot—but not a beer at the local tavern. Or parents could wire to a college student E-money that is designated for rent or books. "There will be new forms of smart money and payment systems that can only be done online," says Myhrvold.

Cover Story

Along with the opportunities, though, comes huge uncertainty. Existing monetary regulations don't cover all of the potential uses of E-cash. Nathaniel S. Borenstein, a computer scientist and co-founder of First Virtual, says: "One of the hardest questions merchants ask us is, 'When do we owe taxes?'" That's not a trivial question: With E-money, the merchant could be in Guam and the buyer in Canada, while First Virtual's computers are located in Ohio. So whose sales tax do you pay? Borenstein's advice to merchants: "I tell them to consult a lawyer."

There's also a major potential for crime (page 78). E-money can be easily sent in and out of a country undetected, facilitating money laundering on a grand scale. Tax evasion could become a matter of pushing a button. And without foolproof cryptography, counterfeiters could replicate the series of digits that constitutes E-money. Governments would be hard pressed to monitor or control stateless E-money. "Digital cash is a threat to every government on the planet that wants to manage its currency," says David E. Saxton, executive vice-president of Net1, a startup that has developed a secure way to send electronic checks across the Internet.

BATTLE OF THE LOGOS. Even law-abiding citizens and companies using E-money could be victims of sophisticated hacker attacks. Says Colin Crook, senior technology officer for Citicorp: "We have to assume electronic money will be the subject of sustained attack from all kinds of people."

Another open question—and a large one—is the role of banks in the new electronic world. "E-cash will be offered by both banks and nonbanks," says Chaum. Sure enough, DigiCash or CyberCash could join forces with AT&T or Microsoft just as easily as with Citibank. Having one of those companies dispensing E-cash directly to consumers could do serious damage to banks' main link with their customers.

Even if banks are involved, they could find other players taking center stage. Early entrants to the E-money business could set the operating standards for digital cash. And the nonbanks could even devise systems that would make their logos the first thing people see. William M. Randle, senior vice-president at Huntington Bancshares, warns that banks could become "buttons on a network operated by other entities."

THE FLEXIBILITY OF CASH

"Imagine it's the same as physical money, and you won't be far off"

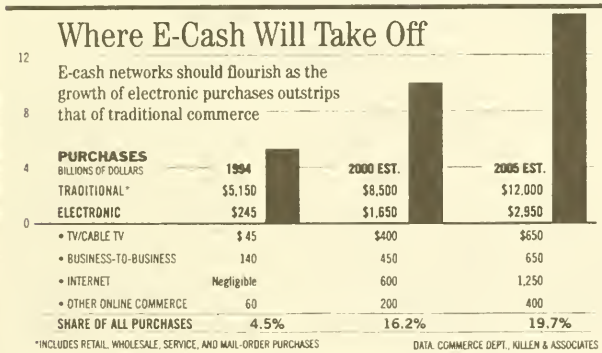
— TIMOTHY JONES, CEO, Mondex

Improbable? Not really. Take a look at credit-card processing. Twenty years ago, banks owned the card-transaction-processing business. Now, close to 80% of card transactions are processed by nonbanks such as First Data Resources Inc., says KPMG's Crone.

A similar erosion has occurred in wholesale banking, where banks have ceded to such outfits as General Electric Information Services and Electronic Data Systems Corp. nearly the entire market for transferring payment data to corporations, leaving themselves the mundane, low-margin service of transferring money between corporations. Today, says banking consultant

Where E-Cash Will Take Off

E-cash networks should flourish as the growth of electronic purchases outstrips that of traditional commerce



PURCHASES BILLIONS OF DOLLARS	1994	2000 EST.	2005 EST.
TRADITIONAL*	$5,150	$8,500	$12,000
ELECTRONIC	$245	$1,650	$2,950
• TV/CABLE TV	$ 45	$400	$650
• BUSINESS-TO-BUSINESS	140	450	650
• INTERNET	Negligible	600	1,250
• OTHER ONLINE COMMERCE	60	200	400
SHARE OF ALL PURCHASES	4.5%	16.2%	19.7%

*INCLUDES RETAIL, WHOLESALE, SERVICE, AND MAIL-ORDER PURCHASES

DATA: COMMERCE DEPT., KILLEN & ASSOCIATES

Cover Story

Edward E. Furash, although the situation is improving, fewer than 100 banks offer full-service electronic data interchange, as the data part of payments transmission is known. "We should do more of that," says Richard Matteis, head of Chemical Banking Corp.'s Geoserve unit.

Banks have one key advantage: a near lock on consumers' trust when it comes to depositing money. For that reason, many bankers tend to dismiss the threat implicit in E-money. "The reason financial institutions are going to win in the long run is trust," says Kawika Daguio, the American Bankers Assn.'s federal representative on operations and banking. Indeed, many E-cash makers are choosing to partner with banks because of that consumer trust. "We've positioned ourselves to work with the banking industry and make sure that if there are heroes in this, it is the banks," says William N. Melton, CEO of CyberCash.

But Microsoft's bid for Intuit last fall gave bankers a collective scare. And even though the deal did not work out, banks worry that Microsoft could hook its 70 million Windows customers into the electronic-commerce networks that

CALL IT E-MONEY MANAGEMENT

It's a Saturday morning sometime in the not-too-distant future, and you sit down at your PC to do a little end-of-the-month planning. First, you call up the balances from your various accounts—credit-card, checking, savings, and E-cash—and break down your spending by category. Oops, better cut down on those pricey dinners.

Your investments are offsetting some of those expensive habits—at least you hope so. Finding out is as easy as a few clicks of a mouse button, as you call up your investment portfolio. Hmmm, it may be time to get into a more aggressive mutual fund. So you quickly dispatch a software "agent" to rustle up profiles for the top-performing funds. By filling out an online form, you transfer some of your holdings into a hot overseas fund.

Just as technology is revolutionizing money, it is also set to transform the way we manage our money. "Complexity has gotten beyond the level that people can deal with," says Scott D. Cook, the founder and chairman of Intuit Inc. With programs like Quicken, Intuit's best-selling personal-finance software, Cook aims to make that complexity easier to deal with.

"AUTOMATIC AGENTS." Indeed, today's programs for personal-finance management and home banking are giving consumers unprecedented control over their financial life. But this is just the beginning. Gradually, programs are linking users to banks, electronic bill-paying services, and a broad array of vendors of financial advice that is starting to be offered online. Colin Crook, head of technology at Citibank, says software programs will be constantly at work for you, for instance, using information gleaned on the Net to optimize your portfolio. "You're going to hand off your personal affairs in cyberspace to automatic agents who represent you," says Crook.

A QUICKENING PACE

"Complexity has gotten beyond the level that people can deal with"

— SCOTT COOK, Chairman, Intuit Inc.

The competition to supply these services will be heated. Microsoft Corp.'s Bill Gates saw the potential—one reason why he was willing to shell out $2 billion for Intuit. With that deal blocked by the Justice Dept., Microsoft is throwing its considerable resources behind Microsoft Money, a home-grown personal-finance package already offered by Chase Manhattan and others. From Money, Microsoft expects to link customers to a variety of online financial services, including electronic bill-paying. Bank of America and NationsBank recently paid $35 million for Meca Software, which makes Managing Your Money. And Intuit, for its part, has just released new programs for selecting mutual funds and planning for retirement and children's college education.

Expect banks to jump into the fray. They are sitting on a gold mine of valuable data: their customers' payment information. The statements they send out, though, typically offer little value, and consumers' credit-card, checking and savings, and investment accounts are handled separately. "There is an opportunity to consolidate that," says Richard K. Crone, a banking consultant at KPMG Peat Marwick.

With so much available to help you manage your financial affairs, someday you may be able to bag those Saturday mornings at the computer and instead just take a long weekend.

By Amy Cortese in New York

it is developing—with or without banks' help. If Microsoft becomes a utility, "it will take a lot of business from the banks," says Montgomery's Fredericks.

Now several of the biggest banks are pushing hard to develop E-money. Citibank's Electronic Monetary System is one of the most advanced bank offerings, although officials there stress that it is still in development. It would allow retail and business customers of Citi—or any other bank that paid to use Citi's system—to convert money in their accounts to electronic cash. Citi customers would also have access to a credit line they could draw down in E-money, just as they would use a credit card. Banks "should be experimenting," says Sholom Rosen, vice-president for electronic commerce at Citi. "That's what we're doing."

Beside NatWest and Midland, Bankers Trust Co. has a group dedicated to electronic commerce. And even some regional banks see opportunities. There is Wells Fargo's work with CyberCash. First Union Corp., based in Charlotte, N.C., has created an electronic mall for Internet transactions. Even Cardinal Bankshares Inc., a $607 million Lexington (Ky.) bank, on May 24 formed a new subsidiary, Security First Network Bank, which aims to grow into a full-service interactive bank on the Internet. "We'll be a one-branch bank in Kentucky with potential customers all over the U.S.," says CEO James S. Mahan III.

While it's not clear who the players will be 10 or even 5 years from now, it is inevitable that much E-money will originate outside the purview of central banks such as the Federal Reserve or the Bank of England, which are largely responsible for traditional monetary regulation. And that has major policy implications.

To begin with, consumers using the stuff could be extremely vulnerable. When consumers lose their credit cards, they are only liable for the first $50 of charges on the card. But for now at least, if a consumer misplaced, say, a Mondex card, it would be like losing cash. Similarly, if your digital coins are stored on the hard drive of your PC, a system crash could wipe out your electronic savings.

Electronic money also creates vast opportunities for tax evasion, money laundering, and other financial crime. "There is an imaginable potential for a serious challenge to the whole political and social order," says First Virtual's Borenstein. "I am not all that sanguine that the government has the control they think they do." For people trying to avoid paying taxes to a national government, the lure of a stateless currency would be powerful indeed. Already, "virtual currencies" serving electronic communities of people are springing up on the Internet.

Then there's the issue of the volatility of money. The effects of high-speed electronic trading have been painfully apparent in market crises over the past several years. Market swings could be magnified if consumers and businesses could send their money around the globe with the touch of a button on a PC.

HIP TO HACKERS' HEISTS

"We have to assume electronic money will be the subject of sustained attack"

— COLIN CROOK, technology chief, Citicorp

The monitoring of national money supplies will also change. While some regulators dismiss the issue, arguing that E-money will inevitably convert back to traditional money and get counted, other experts disagree. Martin Mayer, a guest scholar at the Brookings Institution, says that he expects the Fed to lose control of a significant portion of the money supply.

One of the most pitched debates is likely to be over privacy. As a society, we have relied on a system that allows us to keep some transactions private by using cash, while others, such as big-ticket purchases, are entrusted to a credit-card company or a bank. Competing forms of E-cash offer wildly differing degrees of privacy: DigiCash's E-money offers virtually complete anonymity, while every dollar you spend using the credit-card-based systems would leave a trail. The problem will be balancing individuals' rights to privacy with government's need to monitor money flow and trace criminal activity.

BREAKING INTO THE E-MINT. More dire is the possibility of major break-ins to E-money systems—the electronic equivalent of penetrating the U.S. Mint. If someone were to crack the sophisticated code of, say, the DigiCash system, he could start minting unlimited amounts of his own DigiCash money.

That's why it is all the more alarming that some regulators and even some central bankers still seem unconcerned

with the advent of E-cash. After a breakfast speech to several hundred business leaders in San Francisco last March, Fed Vice-Chairman Alan Blinder was asked whether the Fed is studying the regulatory issues surrounding digital cash. His answer: "Digital what?" Then, after pausing a moment, he added: "It's literally at the thinking stage."

Slowly, though, some regulators are beginning to explore the concept of E-money so they can set policies. The Federal Reserve's payment-systems committee is meeting with Chaum of DigiCash and other E-money pioneers. State tax collectors are looking at the issue of taxing electronic commerce. The Financial Crimes Enforcement Network is also weighing in. Even the White House technology office is taking a big interest.

It's not a moment too soon. "There's no going back," says DigitaLiberty's Frezza. "The genie's out of the bottle. The Internet doesn't have an off switch." And no amount of wishing by regulators will change that.

By Kelley Holland and Amy Cortese in New York, with bureau reports

PATROLLING THE BLACK HOLES OF CYBERSPACE

At first glance, the offer sounded legitimate. First Bank of the Internet began advertising to Net browsers in March, offering a new way to pay for goods over the Net. By sending First Bank a check for at least $20, cybershoppers would get a Visa automated teller machine card "loaded" with their money—less a hefty 5% commission—which they could then use to obtain cash or pay for their cyberwares.

First Bank got numerous inquiries—but it also drew some unwanted scrutiny. State banking regulators warned that it couldn't call itself a bank. The Office of the Comptroller of the Currency sent an advisory to banks and regulators warning them about FBOI. First Bank CEO Vinn K. Beigh, a 34-year-old computer technician in Des Plaines, Ill., says he will soon pull his Net listing. But he is still looking for a way to cash in on the wave of electronic commerce. "There is quite an interest in buying on the Internet," he insists.

He's got that right. First Bank isn't the only upstart trying to cash in on the demand. Consider World Trade Clearinghouse Ltd., which offers a gold-backed cybercurrency with cashlike anonymity that offers "protection from bureaucratic snoops, nasty ex-spouses, and lawsuit-hungry lawyers." And officially opening this month is the Internet Online Offshore Casino, run out of the Turks and Caicos Islands, which says it will accept all manner of E-money and pay customers 10% annual interest on the balances they leave in an offshore bank the company recently bought.

BARBARA RIIS

TANGLES FOR THE TAX MAN

"If you go to a cashless society, it makes it very difficult tracking... reportable income"

— JOHN GIBBONS, President Clinton's top technology adviser

These enterprises may never draw in a meaningful number of customers. And many raise red flags to regulators. But the government is also a long way from getting a good fix on the activities of the much larger number of ostensibly legitimate E-money players.

MONEY LAUNDERERS. The regulatory gaps are sizable. For example, Stanley E. Morris, director of the Treasury Dept.'s Financial Crimes Enforcement Network (FinCEN), points out that there are no laws that limit the balance of electronic currency that can be loaded onto an E-cash card. That could create a major opportunity for money launderers. And no one has determined how to define whose tax laws apply to transactions in cyberspace (page 8). Says John H. Gibbons, assistant to the President for science and technology: "If you go to a cashless society, it makes it very difficult tracking cash income or reportable income.

Right now, regulators are simply trying to understand the new technology and how the market is evolving. Last April, the Federal Trade Commission held a conference to examine the impact of electronic commerce on consumer protection. FinCEN is organizing a colloquium on electronic currency to be held later this fall. "We are nowhere near the issue of regulating it," warns FinCEN's Morris. "We're one step back." Given the speed with which the market is advancing, regulators don't have much time to close that gap.

By Amy Barrett in Washington

Electronic Payment Services, Inc.
1100 Carr Road
Wilmington, Delaware 19809

Table of Contents

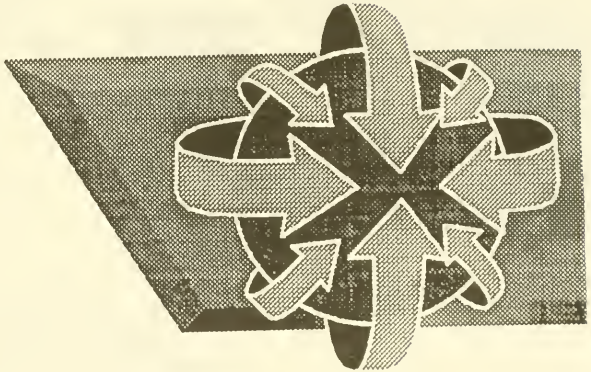
Electronic Payment Services, Inc.

Electronic Payment Services, Inc.

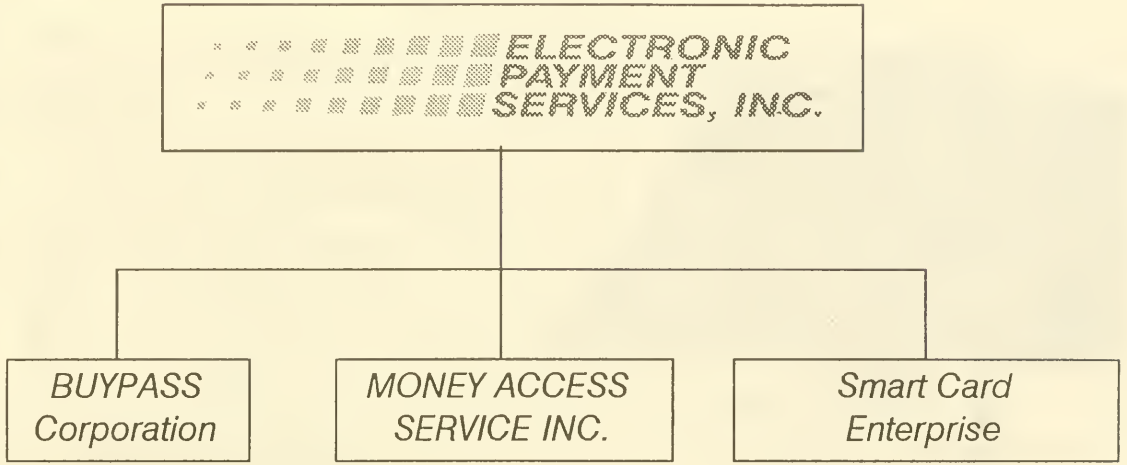
EPS

A joint venture formed to create a for-profit, stand-alone, vertically-integrated business dedicated to the generation of a strong earnings stream through the offering of a broad and comprehensive range of electronic transaction services.

EPS Ownership



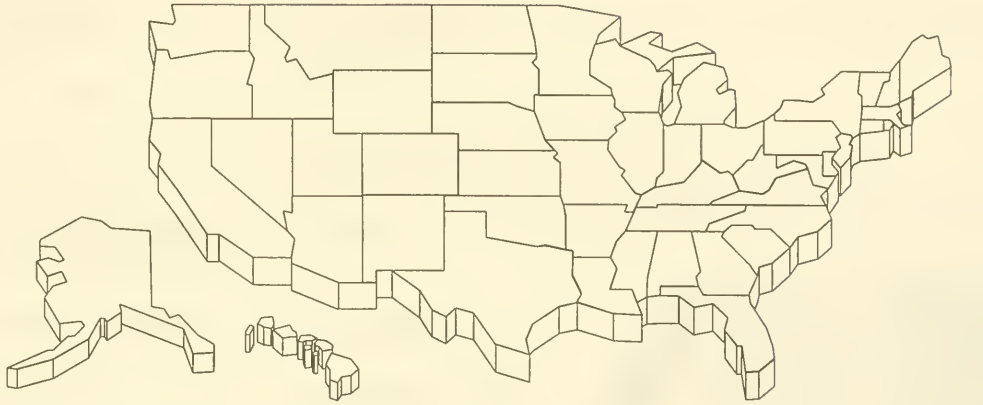
- *Banc One Corporation*
- *CoreStates Financial Corp.*
- *KeyCorp*
- *PNC Bank Corp.*
- *National City Corporation*


ELECTRONIC
PAYMENT
SERVICES, INC.
BUYPASS
Corporation
MONEY ACCESS
SERVICE INC.
Smart Card
Enterprise

EPS Key Facts

Number of Employees	*900*
Formation Date	*December 1992*
Headquarters Location	*Wilmington*
Subsidiary Headquarters:	
- BUYPASS Corporation	*Atlanta*
- MONEY ACCESS SERVICE INC.	*Wilmington*
Processing Sites:	
- BUYPASS	*Atlanta*
- MAC Network	*Wilmington*
- MAC Network	*North Olmsted*

Size and Scope



Processed ATM Transaction Volume	900 Million	Number of Financial Instituions	1,700
Number of ATMs	18,200	Market States ATM / POS	34 / 50
Annual POS Transaction Volume	600 Million	Terminal/Merchant Locations	150,000

The Internet

What is the Internet?

The Internet is a series of computers linked together in a system where each computer (or node) is equal. There is no central authority. Each node has the authority to originate, pass and receive messages.

Internet History

1964-RAND Corporation proposed methodology for successful communication after a nuclear war.

1969-Pentagon funded four nodes using RAND methodolgy calling it the ARPANET.

1971-15 nodes in ARPANET.

1972-37 nodes in ARPANET.

1984-NSF joined ARPANET followed by NASA, NIH and DOE.

Internet History, continued

1989-ARPANET formally expired but standards and protocols remained to connect many computers in many countries.

1995-Tens of thousands of nodes in over 90 countries with possibly 30 million people using the Internet.

Internet Uses

- Mail
- Discussion Groups
- Long-distance computing
- File transfers

?Electronic Commerce

Issues on the Internet

Business people want it put on a sound financial footing.
Government wants it more fully regulated.
Academics want it dedicated to scholarly research.
Military people want it spy-proof and secure.

Electronic Commerce

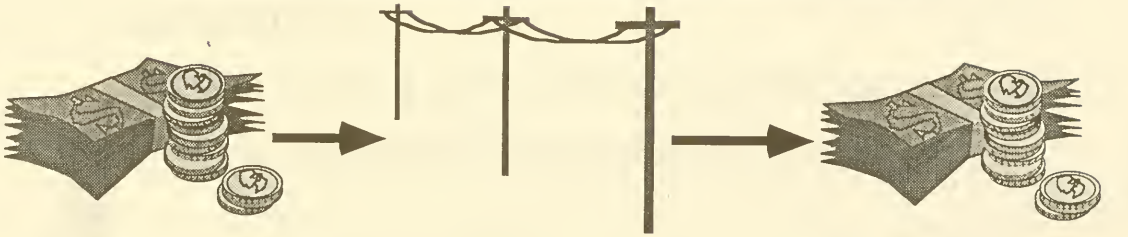
What is Electronic Commerce?

Commerce which takes place using some form of electronic processing, and which is based on a means of value exchange.

United States Coin and Currency are the original form of value exchange santioned by the United States Government.

Government role was to preserve and control the mechanism of value exchange.

Coin and Currency First Used In Electronic Processing Through Wire Transfers



An individual delivers currency to one location and an instruction is sent to another location to disburse an equal amount of currency to an "authenticated" party.

Coin and Currency First Used In Electronic Processing Through Wire Transfers

Issues

Banking Environment

None. A non-bank, Western Union, provided service.

-Security

Privately controlled single purpose transmission facility.

-Authentication

Private system controlled by a single provider; generally a signature system.

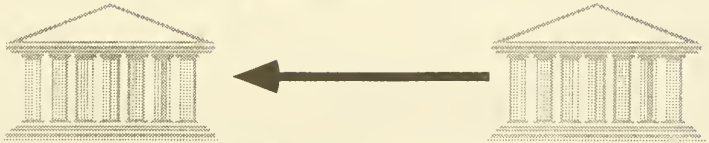
Public Policy

-Privacy

Dedicated privately controlled communications lines not shared with public.

Electronic Purchase Transactions Through Credit Cards

Credit card is given to merchant for purchase. Merchant obtains authorization of transaction electronically. Merchant's bank collects funds from Consumer's bank via a settlement function (i.e. Visa or MasterCard).



Merchant's Bank Consumer's Bank

Electronic Purchase Transactions Through Credit Cards

Issues

Banking Environment

-Security

All transactions within banking system. Safety and soundness standards. Consumers and merchants use banks or third party providers who follow accepted rules.

-Authentication

Bank authorized extensions of credit.

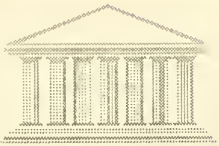
Signature of cardholder.

Public Policy

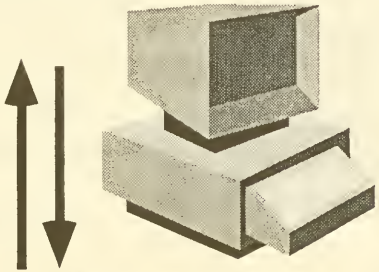
-Privacy

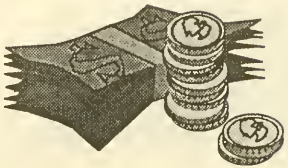
Contained systems; system rules on information disclosure to third parties.

Electronic Cash Withdrawals and Deposits Through Automated Teller Machines



Consumer's Bank





Currency is dispensed and deposited through ATM operated by customer's bank electronically

Electronic Cash Withdrawals and Deposits Through Automated Teller Machines

Issues

Banking Environment

All transactions are between bank and its customer.
Safety and soundness standards applied.

-Security

Electronic signature (PIN) used. Entire transaction is within customer's bank. Monitoring of lines and systems. Dedicated communications lines.

-Authentication

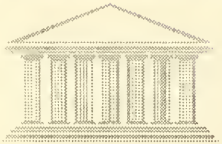
Electronic signature (PIN) used.
Bank authorizes transaction against funds on deposit.

Public Policy

-Privacy

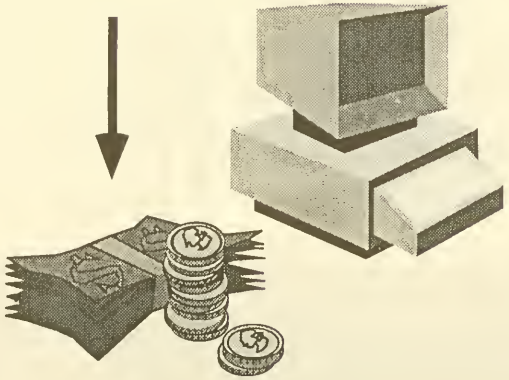
Bank controls all information.

Electronic Cash Withdrawals Through Multiple Banks' ATMs



Bank Where Withdrawal Occurs

Consumer's Bank



Money dispensed through ATM is not consumer's bank. Transfer of funds occurs through a network.

Electronic Cash Withdrawals Through Multiple Banks' ATMs

Issues

Banking Environment

Banks are supervised for safety and soundness. Processors examined for system integrity by Federal regulators.

-Security

Electronic signature (PIN) used. Monitoring of lines and systems. Dedicated communications lines.

-Authentication

Electronic signature (PIN) used.

Public Policy

-Privacy

Federal laws. Bank and processor agreements of confidentiality.

Debit Point of Sale Purchase Transactions

Debit card is given to merchant for purchase. Merchant authorizes amount electronically. Merchant's bank collects funds from Consumer's DDA account.

Merchant's Bank

Consumer's DDA Account

Debit Point of Sale Purchase Transactions

Issues

Banking Environment

Banks are supervised for safety and soundness. Processors examined for system integrity by Federal regulators. All parties maintain bank accounts and funds are transmitted interbank.

-Security

Encrypted electronic signatures (PINs) used. PIN pads and terminals are tamper proof. Dedicated communications lines used often.

-Authentication

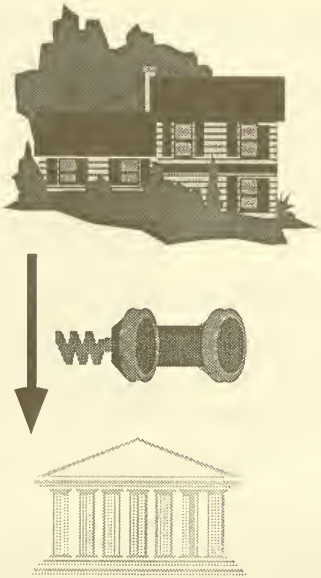
Electronic signature (PIN) used.

Public Policy

-Privacy

Network rules. Agreements of confidentiality and law.

Home Banking



Consumer can perform "electronic" banking through either a telephone line or a computer. Initially, this was confined to consumer's own bank.

Consumer's Bank

Home Banking

Issues

Banking Environment

Banks are supervised for safety and soundness.

-Security

Single bank only; password different from electronic signatures. Only balance information or account transfers occur.

-Authentication

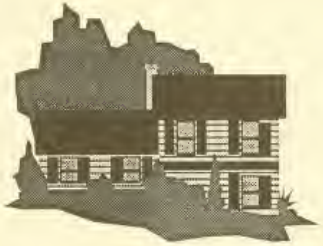
Password is used and changeable by customer at will.

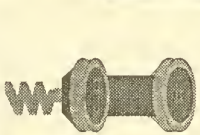
Public Policy

-Privacy

All information exchange deals only with moving funds between accounts at single bank. All information remains within bank. No major issue here.

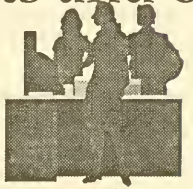
Expanded Home Banking





Consumer can perform "electronic" banking through either a telephone line or a computer, including moving funds to pay bills to merchants and others.

Consumer's Bank



Merchant

Expanded Home Banking

Issues

Banking Environment

Banks are supervised for safety and soundness. Funds move from bank after authorization. All payments remain in banking system.

-Security

Use of changeable password.

Authorization of payment by bank against funds on deposit.

-Authentication

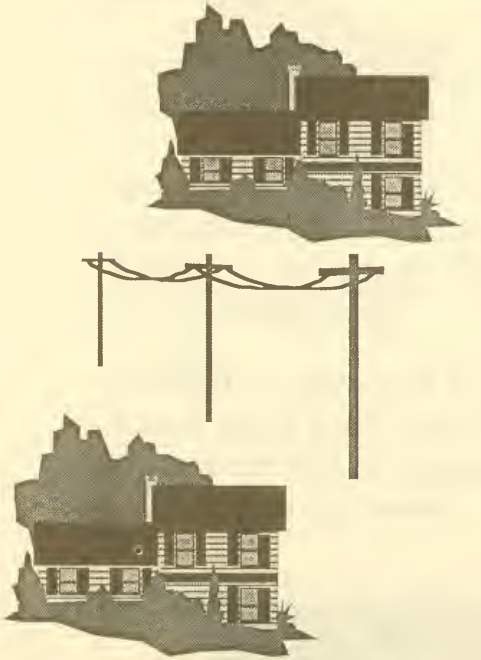
By password; Bank must authorize payment.

Public Policy

-Privacy

All instructions are between customer and bank who then pays merchant.

Commerce on the Internet
Further Expanded Home Banking

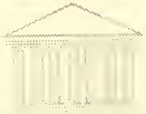


An individual buys something from another individual or merchant over the Internet. Role of banks and U.S. government is unclear.

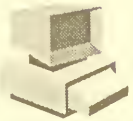
Commerce on the Internet Stakeholders

Consumers

Merchants



Financial Institutions



Providers (i.e. Visa, MasterCard, Microsoft, Intuit, CyberCash, Digicash)

Government

Commerce on the Internet Issues

-System Integrity
-Safety and Soundness of Providers
-Regulation of Providers or Examination
-Security
-Authentication
-Privacy
-Money Supply
  -Tracking Amount
  -Velocity
-Taxation
-Tracking Transactions
-Audit
-Liabilities
  -Fraud
  -System downtime
-Consumers: Fraudulant Transactions
-Applicable laws

Issues

Electronic Commerce-Issues

	Credit Cards	ATMs	Debit POS	Home Banking	Internet
System Integrity	X	X	X	X	?
Safety & Soundness	X	X	X	X	?
Regulation-Providers	X	X	X	X	?
Security	X	X	X	X	?
Authentication	X	X	X	X	?
Privacy	X	X	X	X	?
Money Supply					
-Tracking Amount	X	X	X	X	?
-Velocity	X	X	X	X	?
Taxation	X	X	X	X	?
Tracking Transactions	X	X	X	X	?
Audit	X	X	X	X	?
Liabilities					
-Fraud	X	X	X	X	?
-System downtime	X	X	X	X	?
Consumers: Fraud	X	X	X	X	?
Applicable laws	X	X	X	X	?

Testimony by Dr. David Chaum

Chairman and Chief Executive Officer

DigiCash, Inc.

"The Future of Money"

Before the

Subcommittee on Domestic and International Monetary Policy

of the

Committee on Banking and Financial Services

United States House of Representatives

July 25, 1995

Mr. Chairman, Members of the Committee:

As an American who is regarded as the inventor of electronic cash, who has worked over the last dozen or so years to make the technology viable, and who is now CEO of a leading company pioneering in its commercialization, I am very pleased by the interest being shown here and to be here today.

We are being forced to decide between two very different kinds of electronic payment technology. The core values we as a nation have fought for, and continue to stand for, are at stake. As a consequence of choosing one of the two directions, these values will be profoundly eroded; by choosing the other direction, however, they will be preserved and likely extended. Wise decisions at this critical juncture may also allow us to avoid certain other pitfalls and to realize economic leadership and growth.

I think my limited time before you is best used to briefly explain the fundamentally different approaches to security, before coming to privacy, privacy technology, and its implications.

Security

Security is simply the protection of interests. People want to protect their own money and banks their own exposure. The role of government is to maintain the integrity of, and confidence in, the whole system. With electronic cash, just as with paper cash today, it will be the responsibly of government to protect against systemic risk. This is a serious role that cannot be left to the micro-economic interests of commercial organizations.

In order for those in government to make informed decisions, it will be necessary for them to understand the basic ways to secure transactions in different situations.

One basic form is tamper-resistance, exemplified by the chip in a chip card. It is designed to be hard to modify or to read secrets from. Such tamper-resistance is needed for "off-line" payments—those in which the reader device receiving payment from a card, validates payments by contacting a central system only at the end of each day.

(Incidentally, this and the other basic form must rely for security on cryptography, sometimes refereed to as encryption, which is fundamental to all information security.)

The other basic form is where the individual uses their own computer, whether a desk-top, lap-top, or palm-top device. Such "software only" is all that is needed in an "on-line" system—a system in which the party receiving payment communicates over a network during each payment.

The trend is toward a convergence of these two forms into a hybrid—since people don't want incompatible forms of money and since it offers the best of both worlds in terms of convenience; in other words, you will put a chip card into a user-friendly electronic device of your own choosing, whether on your desk, in your living room, or in you pocket. I have brought some examples of this to show you...

The problems I see in the industry today reflect a lack architecture. And architecture is essential when building infrastructure, which is what we are embarking on. In my view, a sound architecture must: (i) include the two basic forms of security, and allow for their integration into the hybrid; (ii) prevent the vulnerability of system-wide secrets from being stored in every card or, nearly as bad, every off-line point of payment; and (iii) address privacy concerns effectively, since they cannot be addressed as add-ons or afterthoughts. Today, DigiCash systems are alone in having any of these three attributes, and their architecture has all three.

Privacy

Let me now turn to this issue of privacy...

A recent Harris pole of the American public began by introducing respondents to all the consumer benefits of the information superhighway. Then respondents were told that in order to make such systems economically viable, payment transaction data would have to be gathered and used for purposes such as making special offers to them. But the majority of respondents still objected to any use, other than consummation of the payment, and they gave privacy as the primary reason.

Fully 82% of Americans today expressed concern over privacy of computerized data. That fraction has been growing steadily ever since the "first wave" of privacy concern was triggered when Americans saw their names punched into computer cards or printed on computer generated forms. When people are exposed to the information superhighway, which provides an awesome glimpse of the power of modern information technology, with dropping transaction costs leading to finer granularity of payments (which we will be hearing more about later), concern will reach new levels.

Privacy Technology

"Privacy technology" allows people to protect their own information, and other interests, while at the same time it maintains very high security for organizations. Essentially, it is the difference between, on the one hand, a centralized system with disenfranchised participants (like the electronically tagged animals in feedlots); and, on the other hand, a system where each participant is able to protect its own interests (like buyers and sellers on a town market square).

Take ecash as an example of privacy technology. It provides a fully digital bearer instrument—a number that is itself money, just like a bank note is money. On the Internet, once someone downloads the requisite software, which takes only a few minutes, they are ready to send and receive ecash in payments.

Security of ecash is superior to that of paper cash. If it is stolen, it cannot be used: if someone refuses to give you a receipt, you have proof that they deposited it; and if it is lost, you can get your money and records back. Counterfeiting ecash poses the same cryptographic challenge as breaking the most sophisticated codes used to protect nuclear materials, military secrets and large-value wire transfers. Therefore, ecash is certainly not the target of opportunity.

Ecash is already being experimented with on the Internet in a worldwide monopoly money trial with tens of thousands of participants. Related card technology has been extensively tested, by DigiCash licensee Amtech, for highway-speed road tolls and road pricing, offering privacy instead of dossiers on everywhere people drive. And, CAFE, the European Commission sponsored trial, at its headquarters buildings in Brussels, of chip cards that can be inserted into electronic wallets (that I have already shown you), allows privacy in payments and the electronic ECU. Such "privacy technology" was even successfully used by the participants at the most recent international meeting of data protection commissioners.

Ecash has received substantial media coverage; consequently, the public is beginning to realize that the coming of electronic payments need not mean an obliteration of privacy. And the superhighway will give consumers unprecedented mobility to choose it.

Some concern about ecash, however, has been raised by various parties over possibilities it might open for illicit payments. But there is simply no legitimate basis for these allegations.

Ecash, even when it achieves significant scale, is considerably less dangerous to society than automatic teller machines. For one thing, like cash, the amount withdrawn and deposited is on record; but, for another, unlike cash, the amounts of money that pass through each person's hands all also on record at the bank. Ecash itself is less prone to abuse than paper bank notes, because privacy is "one-way," which means that an extortionist, a seller on a black-market, or the acceptor of a bribe is forever vulnerable to being irrefutably incriminated by the party that paid them.

National Leadership

Governments who stifle the new technology while it is still in its infancy, before its has had a chance to develop and harmonize with our institutions; who don't pro-actively support needed infrastructure; or who fail to establish confidence by protecting against systemic risk—will be left behind in global competition. Countries who take clear positions based on understanding of the technology, however, and encourage needed developments, stand to gain enormous economic growth and market leadership. Privacy technology, whether used for electronic payments, voting, or other public expression, is the electronic equivalent of a free market and democracy. People will come to insist on it as an informational human right.

Achieving Electronic Privacy

A cryptographic invention known as a blind signature permits numbers to serve as electronic cash or to replace conventional identification. The author hopes it may return control of personal information to the individual

by David Chaum

Every time you make a telephone call, purchase goods using a credit card, subscribe to a magazine or pay your taxes, that information goes into a data base somewhere. Furthermore, all these records can be linked so that they constitute in effect a single dossier on your life—not only your medical and financial history but also what you buy, where you travel and whom you communicate with. It is almost impossible to learn the full extent of the files that various organizations keep on you, much less to assure their accuracy or to control who may gain access to them.

Organizations link records from different sources for their own protection. Certainly it is in the interest of a bank looking at a loan application to know that John Doe has defaulted on four similar loans in the past two years. The bank's possession of that information also helps its other customers, to whom the bank passes on the cost of bad loans. In addition, these records permit Jane Roe, whose payment history is impeccable, to establish a charge account at a shop that has never seen her before.

That same information in the wrong hands, however, provides neither protection for businesses nor better service for consumers. Thieves routinely use a stolen credit card number to trade on their victims' good payment records; murderers have tracked down their targets by consulting government-maintained address records. On another level, the U.S. Internal Revenue Service has attempted to single out taxpayers for audits based on estimates of household income compiled by mailing-list companies.

The growing amounts of information that different organizations collect about a person can be linked because all of them use the same key—in the U.S. the social security number—to identify the individual in question. This identifier-based approach perforce trades off security against individual liberties. The more information that organizations have (whether the intent is to protect them from fraud or simply to target marketing efforts), the less privacy and control people retain.

Over the past eight years, my colleagues and I at CWI (the Dutch nationally funded Center for Mathematics and Computer Science in Amsterdam) have developed a new approach, based on fundamental theoretical and practical advances in cryptography, that makes this trade-off unnecessary. Transactions employing these techniques avoid the possibility of fraud while maintaining the privacy of those who use them.

In our system, people would in effect give a different (but definitively verifiable) pseudonym to every organization they do business with and so make dossiers impossible. They could pay for goods in untraceable electronic cash or present digital credentials that serve the function of a banking passbook, driver's license or voter registration card without revealing their identity. At the same time, organizations would benefit from increased security and lower record-keeping costs.

Recent innovations in microelectronics make this vision practical by providing personal "representatives" that store and manage their owners' pseudonyms, credentials and cash. Microprocessors capable of carrying out the necessary algorithms have already been embedded in pocket computers the size and thickness of a credit card. Such systems have been tested on a small scale and could be in widespread use by the middle of this decade.

The starting point for this approach is the digital signature, first proposed in 1976 by Whitfield Diffie, then at Stanford University. A digital signature transforms the message that is signed so that anyone who reads it can be sure of who sent it [see "The Mathematics of Public-Key Cryptography," by Martin E. Hellman; SCIENTIFIC AMERICAN, August 1979]. These signatures employ a secret key used to sign messages and a public one used to verify them. Only a message signed with the private key can be verified by means of the public one. Thus, if Alice wants to send a signed message to Bob (these two are the cryptographic community's favorite hypothetical characters), she transforms it using her private key, and he applies her public key to make sure that it was she who sent it. The best methods known for producing forged signatures would require many years, even using computers billions of times faster than those now available.

To see how digital signatures can provide all manner of unforgeable credentials and other services, consider how they might be used to provide an electronic replacement for cash. The First Digital Bank would offer electronic bank notes: messages signed using a particular private key. All messages bearing one key might be worth a dollar, all those bearing a different key five dollars, and so on for whatever denominations were needed. These electronic bank notes could be authenticated using the corresponding public key, which the bank has made a matter of record. First Digital would also make public a key to authenticate electronic documents

DAVID CHAUM is head of the Cryptography Group at the Center for Mathematics and Computer Science (CWI) in Amsterdam. He is also a founder of DigiCash, which develops electronic payment systems. Chaum received his Ph.D. in computer science from the University of California, Berkeley, in 1982 and joined CWI in 1984. He helped to found the International Association for Cryptologic Research and remains active on its board; he also consults internationally on cryptology.

sent from the bank to its customers.

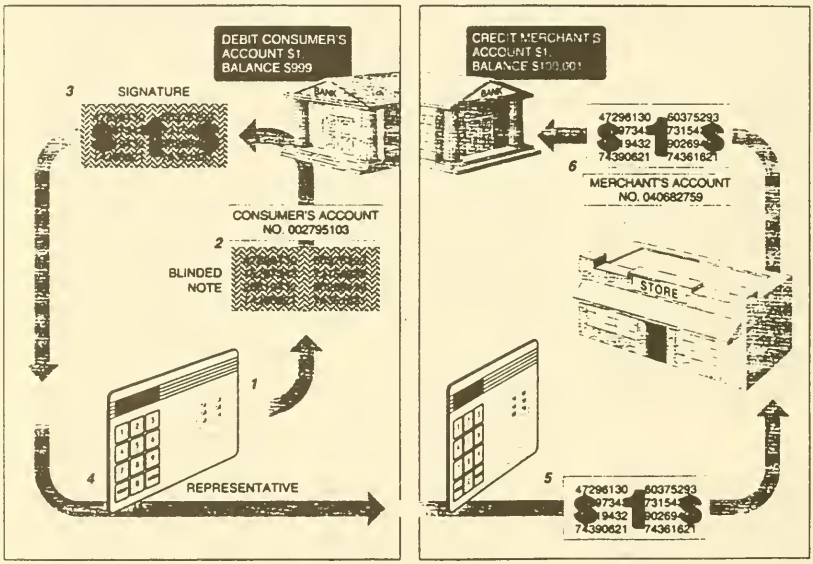
To withdraw a dollar from the bank, Alice generates a note number (each note bears a different number, akin to the serial number on a bill); she chooses a 100-digit number at random so that the chance anyone else would generate the same one is negligible. She signs the number with the private key corresponding to her "digital pseudonym" (the public key that she has previously established for use with her account). The bank verifies Alice's signature and removes it from the note number, signs the note number with its worth-one-dollar signature and debits her account. It then returns the signed note along with a digitally signed withdrawal receipt for Alice's records. In practice, the creation, signing and transfer of note numbers would be carried out by Alice's card computer. The power of the cryptographic protocols, however, lies in the fact that they are secure regardless of physical medium: the same transactions could be carried out using only pencil and paper.

When Alice wants to pay for a purchase at Bob's shop, she connects her "smart" card with his card reader and transfers one of the signed note numbers the bank has given her. After verifying the bank's digital signature, Bob transmits the note to the bank, much as a merchant verifies a credit card transaction today. The bank reverifies its signature, checks the note against a list of those already spent and credits Bob's account. It then transmits a "deposit slip," once again unforgeably signed with the appropriate key. Bob hands the merchandise to Alice along with his own digitally signed receipt, completing the transaction.

This system provides security for all three parties. The signatures at each stage prevent any one from cheating either of the others: the shop cannot deny that it received payment, the bank cannot deny that it issued the notes or that it accepted them from the shop for deposit, and the customer can neither deny withdrawing the notes from her account nor spend them twice.

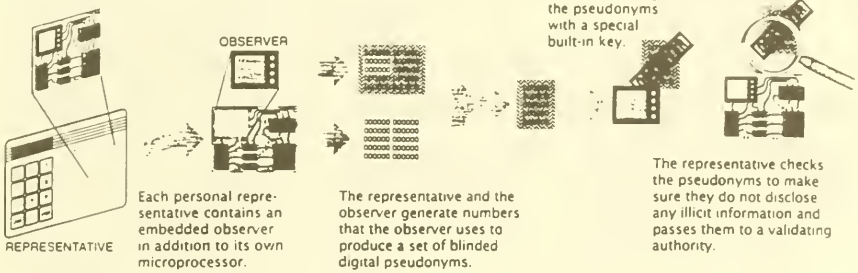
This system is secure, but it has no privacy. If the bank keeps track of note numbers, it can link each shop's deposit to the corresponding withdrawal and so determine precisely where and when Alice (or any other account holder) spends her money. The resulting dossier is far more intrusive than those now being compiled. Furthermore, records based on digital signatures are more vulnerable to abuse than conventional files. Not only are they self-authenticating (even if they are copied, the information they contain can be verified by anyone), but they also permit a person who has a particular kind of information to prove its existence without either giving the information away or revealing its source. For example, someone might be able to prove incontrovertibly that Bob had telephoned Alice on 12 separate occasions without having to reveal the time and place of any of the calls.

I have developed an extension of digital signatures, called blind signatures, that can restore privacy. Before send-



DIGITAL CASH flows tracelessly from bank through consumer and merchant before returning to the bank. Using a small computer "representative," a person creates a random number to serve as a bank note. The bank debits the appropriate account and signs the note with an unforgeable digital signature indicating its value. The bank credits the merchant's account when the note is presented for payment. A technique known as a blind signature prevents the bank from seeing the note number so the bank will be unable to correlate withdrawals from one account with deposits to another.

How to Create Secure Digital Pseudonyms



ing a note number to the bank for signing, Alice in essence multiplies it by a random factor. Consequently, the bank knows nothing about what it is signing except that it carries Alice's digital signature. After receiving the blinded note signed by the bank, Alice divides out the blinding factor and uses the note as before.

The blinded note numbers are "unconditionally untraceable"—that is, even if the shop and the bank collude, they cannot determine who spent which notes. Because the bank has no idea of the blinding factor, it has no way of linking the note numbers that Bob deposits with Alice's withdrawals. Whereas the security of digital signatures is dependent on the difficulty of particular computations, the anonymity of blinded notes is limited only by the unpredictability of Alice's random numbers. If she wishes, however, Alice can reveal these numbers and permit the notes to be stopped or traced.

Blinded electronic bank notes protect an individual's privacy, but because each note is simply a number, it can be copied easily. To prevent double spending, each note must be checked on-line against a central list when it is spent. Such a verification procedure might be acceptable when large amounts of money are at stake, but it is far too expensive to use when someone is just buying a newspaper. To solve this problem, my colleagues Amos Fiat and Moni Naor and I have proposed a method for generating blinded notes that requires the payer to answer a random numeric query about each note when making a payment. Spending such a note once does not compromise unconditional untraceability, but spending it twice reveals enough information to make the payer's account easily traceable. In fact, it can yield a digitally signed confession that cannot be forged even by the bank.

Cards capable of such anonymous payments already exist. Indeed, DigiCash, a company with which I am associated, has installed equipment in two office buildings in Amsterdam that permits copiers, fax machines, cafeteria cash registers and even coffee vending machines to accept digital "bank notes." We have also demonstrated a system for automatic toll collection in which automobiles carry a card that responds to radioed requests for payment even as they are traveling at highway speeds.

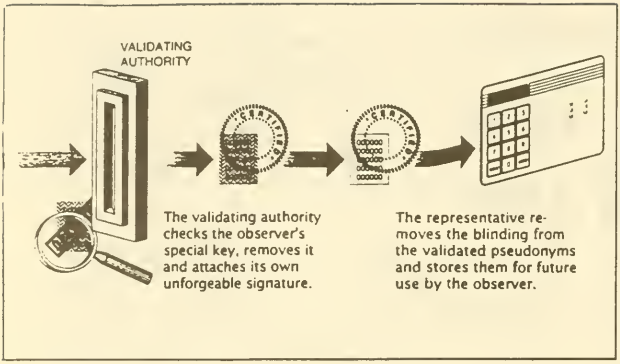
My colleagues and I call a computer that handles such cryptographic transactions a "representative." A person might use different computers as representatives depending on which was convenient: Bob might purchase software (transmitted to him over a network) by using his home computer to produce the requisite digital signatures, go shopping with a "palm-top" personal computer and carry a smart credit card to the beach to pay for a drink or crab cakes. Any of these machines could represent Bob in a transaction as long as the digital signatures each generates are under his control.

Indeed, such computers can act as representatives for their owners in virtually any kind of transaction. Bob can trust his representative and Alice hers because they have each chosen their own machine and can reprogram it at will (or, in principle, build it from scratch). Organizations are protected by the cryptographic protocol and so do not have to trust the representatives.

The prototypical representative is a smart credit-card-size computer containing memory and a microprocessor. It also incorporates its own keypad and display so that its owner can control the data that are stored and exchanged. If a shop provided the keypad and display, it could intercept passwords on their way to the card or show one price to the customer and another to the card. Ideally, the card would communicate with terminals in banks and shops by a short-range communications link such as an infrared transceiver and so need never leave its owner's hands.

When asked to make a payment, the representative would present a summary of the particulars and await approval before releasing funds. It would also insist on electronic receipts from organizations at each stage of all transactions to substantiate its owner's position in case of dispute. By requiring a password akin to the PIN (personal identifying number) now used for bank cards, the representative could safeguard itself from abuse by thieves. Indeed, most people would probably keep backup copies of their keys, electronic bank notes and other data; they could recover their funds if a representative were lost or stolen.

Personal representatives offer excellent protection for individual privacy, but organizations might prefer a mechanism to protect their interests as strongly as possible. For example, a bank might want to prevent double spending of bank notes altogether rather than



simply detecting it after the fact. Some organizations might also want to ensure that certain digital signatures are not copied and widely disseminated (even though the copying could be detected afterward).

Organizations have already begun issuing tamperproof cards (in effect, their own representatives) programmed to prevent undesirable behavior. But these cards can act as "Little Brothers" in everyone's pocket.

We have developed a system that satisfies both sides. An observer—a tamper-resistant computer chip, issued by some entity that organizations can trust—acts like a notary and certifies the behavior of a representative in which it is embedded. Philips Industries has recently introduced a tamper-resistant chip that has enough computing power to generate and verify digital signatures. Since then, Siemens, Thomson CSF and Motorola have announced plans for similar circuits, any of which could easily serve as an observer.

The central idea behind the protocol for observers is that the observer does not trust the representative in which it resides, nor does the representative trust the observer. Indeed, the representative must be able to control all data passing to or from the observer; otherwise the tamperproof chip might be able to leak information to the world at large.

When Alice first acquires an observer, she places it in her smart-card representative and takes it to a validating authority. The observer generates a batch of public and private key pairs from a combination of its own random numbers and numbers supplied by the card. The observer does not reveal its numbers but reveals enough information about them so that the card can later check whether its numbers were in fact used to produce the resulting keys. The card also produces random data that the observer will use to blind each key.

Then the observer blinds the public keys, signs them with a special built-in key and gives them to the card. The card verifies the blinding and the signature and checks the keys to make sure they were correctly generated. It passes the blinded, signed keys to the validating authority, which recognizes the observer's built-in signature, removes it and signs the blinded keys with its own key. The authority passes the keys back to the card, which unblinds them. These keys, bearing the signature of the validating authority, serve as digital pseudonyms for future transactions; Alice can draw on them as needed.

An observer could easily prevent (rather than merely detect) double spending of electronic bank notes. When Alice withdraws money from her bank, the observer witnesses the process and so knows what notes she received. At Bob's shop, when Alice hands over a note from the bank, she also hands over a digital pseudonym (which she need use only once) signed by the validating authority. Then the observer, using the secret key corresponding to the validated pseudonym, signs a statement certifying that the note will be spent only once, at Bob's shop and at this particular time and date. Alice's card verifies the signed statement to make sure that the observer does not leak any information and passes it to Bob. The observer is programmed to sign only one such statement for any given note.

Many transactions do not simply require a transfer of money. Instead they involve credentials—information about an individual's relationship to some organization. In today's identifier-based world, all of a person's credentials are easily linked. If Alice is deciding whether to sell Bob insurance, for example, she can use his name and date of birth to gain access to his credit status, medical records, motor vehicle file and criminal record, if any.

Using a representative, however, Bob would establish relationships with different organizations under different digital pseudonyms. Each of them can recognize him unambiguously, but none of their records can be linked.

In order to be of use, a digital credential must serve the same function as a paper-based credential such as a driver's license or a credit report. It must convince someone that the person attached to it stands in a particular relation to some issuing authority. The name, photograph, address, physical description and code number on a driver's license, for example, serve merely to link it to a particular person and to the corresponding record in a data base. Just as a bank can issue unforgeable, untraceable electronic cash, so too could a university issue signed digital diplomas or a credit-reporting bureau issue signatures indicating a person's ability to repay a loan.

When the young Bob graduates with honors in medieval literature, for example, the university registrar gives his representative a digitally signed message asserting his academic credentials. When Bob applies to graduate school, however, he does not show the admissions committee that message. Instead his representative asks its observer to sign a statement that he has a B.A. cum laude and that he qualifies for financial aid based on at least one of the university's criteria (but without revealing which ones). The observer, which has verified and stored each of Bob's credentials as they come in, simply checks its memory and signs the statement if it is true.

In addition to answering just the right question and being more reliable than paper ones, digital credentials would be both easier for individuals to obtain and to show and cheaper for organizations to issue and to authenticate. People would no longer need to fill out long and revealing forms. In-

stead their representatives would convince organizations that they meet particular requirements without disclosing any more than the simple fact of qualification. Because such credentials reveal no unnecessary information, people would be willing to use them even in contexts where they would not willingly show identification, thus enhancing security and giving the organization more useful data than it would otherwise acquire.

Positive credentials, however, are not the only kind that people acquire. They may also acquire negative credentials, which they would prefer to conceal: felony convictions, license suspensions or statements of pending bankruptcy. In many cases, individuals will give organizations the right to inflict negative credentials on them in return for some service. For instance, when Alice borrows books from a library, her observer would be instructed to register an overdue notice unless it had received a receipt for the books' return within some fixed time.

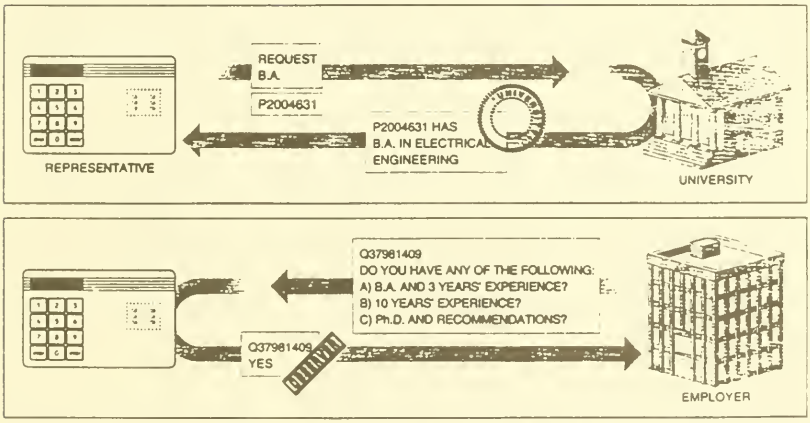
Once the observer has registered a negative credential, an organization can find out about it simply by asking the observer (through the representative) to sign a message attesting to its presence or absence. Although a representative could muzzle the observer, it could not forge an assertion about the state of its credentials. In other cases, organizations might simply take the lack of a positive credential as a negative one. If Bob signs up for skydiving lessons, his instructors may assume that he is medically unfit unless they see a credential to the contrary.

For most credentials, the digital signature of an observer is sufficient to convince anyone of its authenticity. Under some circumstances, however, an organization might insist that an observer demonstrate its physical presence. Otherwise, for example, any number of people might be able to gain access to nontransferable credentials (perhaps a health club membership) by using representatives connected by concealed communications links to another representative containing the desired credential.

Moreover, the observer must carry out this persuasion while its input and output are under the control of the representative that contains it. When Alice arrives at her gym, the card reader at the door sends her observer a series of single-bit challenges. The observer immediately responds to each challenge with a random bit that is encoded by the card on its way back to the organization. The speed of the observer's response establishes that it is inside the card (since processing a single bit introduces almost no delay compared with the time that signals take to traverse a wire). After a few dozen interactions the card reveals to the observer how it encoded the responses; the observer signs a statement including the challenges and encoded responses only if it has been a party to that challenge-response sequence. This process convinces the organization of the observer's presence without allowing the observer to leak information.

Organizations can also issue credentials using methods that depend on cryptography alone rather than on observers. Although currently practical approaches can handle only relatively simple queries, Gilles Brassard of the University of Montreal, Claude Crépeau of the École Normale Supérieure and I have shown how to answer arbitrary combinations of questions about even the most complex credentials while maintaining unconditional unlinkability. The concealment of purely cryptographic negative credentials could be detected by the same kinds of techniques that detect double spending of electronic bank notes. And a combination of these cryptographic methods with observers would offer accountability after the fact even if the observer chip were somehow compromised.

The improved security and privacy of digital pseudonyms exact a price: responsibility. At present, for example, people can disavow credit card purchases made over the tele-



DIGITAL CREDENTIALS put personal information under the control of an individual's representative and its observer. When Alice (one of the author's two hypothetical characters) finishes her undergraduate work, the university gives her a digitally signed degree. Later, her observer can use its knowledge of the degree to answer questions about her qualifications without revealing any more information about her than absolutely necessary.

phone or cash withdrawals from an automatic teller machine (ATM). The burden of proof is on the bank to show that no one else could have made the purchase or withdrawal. If computerized representatives become widespread, owners will establish all their own passwords and so control access to their representatives. They will be unable to disavow a representative's actions.

Current tamper-resistant systems such as ATMs and their associated cards typically rely on weak, inflexible security procedures because they must be used by people who are neither highly competent nor overly concerned about security. If people supply their own representatives, they can program them for varying levels of security as they see fit. (Those who wish to trust their assets to a single four-digit code are free to do so, of course.) Bob might use a short PIN (or none at all) to authorize minor transactions and a longer password for major ones. To protect himself from a robber who might force him to give up his passwords at gunpoint, he could use a "duress code" that would cause the card to appear to operate normally while hiding its more important assets or credentials or perhaps alerting the authorities that it had been stolen.

A personal representative could also recognize its owner by methods that most people would consider unreasonably intrusive in an identifier-based system; a notebook computer, for example, might verify its owner's voice or even fingerprints. A supermarket checkout scanner capable of recognizing a person's thumbprint and debiting the cost of groceries from their savings account is Orwellian at best. In contrast, a smart credit card that knows its owner's touch and doles out electronic bank notes is both anonymous and safer than cash. In addition, incorporating some essential part of such identification technology into the tamper-proof observer would make such a card suitable even for very high security applications.

Computerized transactions of all kinds are becoming ever more pervasive. More than half a dozen countries have developed or are testing chip cards that would replace cash. In Denmark, a consortium of banking, utility and transport companies has announced a card that would replace coins and small bills; in France, the telecommunications authorities have proposed general use of the smart cards now used at pay telephones. The government of Singapore has requested bids for a system that would communicate with cars and charge their smart cards as they pass various points on a road (as opposed to the simple vehicle identification systems already in use in the U.S. and elsewhere). And cable and satellite broadcasters are experimenting with smart cards for delivering pay-per-view television. All these systems, however, are based on cards that identify themselves during every transaction.

COMPUTERIZED CREDIT CARD developed by Toshiba and Visa International contains a microprocessor, memory, keypad and display. Although this card identifies its user during transactions, the same hardware could be reprogrammed as a personal representative for spending digital cash.

If the trend toward identifier-based smart cards continues, personal privacy will be increasingly eroded. But in this conflict between organizational security and individual liberty, neither side emerges as a clear winner. Each round of improved identification techniques, sophisticated data analysis or extended linking can be frustrated by widespread noncompliance or even legislated limits, which in turn may engender attempts at further control.

Meanwhile, in a system based on representatives and observers, organizations stand to gain competitive and political advantages from increased public confidence (in addition to the lower costs of pseudonymous record-keeping). And individuals, by maintaining their own cryptographically guaranteed records and making only necessary disclosures, will be able to protect their privacy without infringing on the legitimate needs of those with whom they do business.

The choice between keeping information in the hands of individuals or of organizations is being made each time any government or business decides to automate another set of transactions. In one direction lies unprecedented scrutiny and control of people's lives, in the other, secure parity between individuals and organizations. The shape of society in the next century may depend on which approach predominates.

FURTHER READING

SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE. David Chaum in *Communications of the ACM*, Vol. 28, No. 10, pages 1030–1044, October 1985.

THE DINING CRYPTOGRAPHERS PROBLEM: UNCONDITIONAL SENDER AND RECIPIENT UNTRACEABILITY. David Chaum in *Journal of Cryptology*, Vol. 1, No. 1, pages 65–75; 1988.

MODERN CRYPTOLOGY: A TUTORIAL. Gilles Brassard in *Lecture Notes in Computer Science*, Vol. 325. Springer-Verlag, 1988.

PRIVACY PROTECTED PAYMENTS: UNCONDITIONAL PAYER AND/OR PAYEE UNTRACEABILITY. David Chaum in *Smart Card 2000: The Future of IC Cards*. Edited by David Chaum and Ingrid Schaumüller-Bichl. North-Holland, 1989.

Testimony of William N. Melton,
CEO, CyberCash Inc.
delivered to the
House Committee on Banking and Financial Services
Subcommittee on Domestic and International Monetary Policy
Hon. Michael N. Castle, Chairman

Hearing on the Future of Money and Payment Systems
July 25, 1995, 10:00 a.m.

My name is Bill Melton. I am President/CEO of CyberCash.

The explosive growth of the Internet carries with it the potential for wholly new electronic payment systems. For the first time, the average American citizen is able to communicate instantaneously, at a negligible cost, with somewhere between 30 and 50 million other people, all over the world. In this new electronic world, geography and national boundaries become irrelevant. People will travel and shop around the planet without regard to distance, time of day or location. And because people will be buying and selling things in this new electronic world, payment systems will evolve to support them. The potential even exists for an entirely new monetary system in cyberspace, one that transcends national governments and national boundaries.

But monetary systems are ultimately founded on trust--trust that your money will be there when you want it, and its value will remain relatively stable. That trust exists now in the three-dimensional world because of a strong global banking system backed by stable national governments. And we at CyberCash believe that commerce on the Internet will be best served by facilitating the transition of existing payment systems--and the trust that is carried with them--into cyberspace. While new payment systems and new monetary systems may ultimately evolve in the future, CyberCash believes that the best way to get there is build on the trust that already exists in the present monetary system.

Accordingly, CyberCash builds technology tools for banks and credit card associations. Our technology tools facilitate the use of a variety of payment instruments on the Internet. Our focus is primarily consumer payment instruments, including credit cards and checks.

Of course our technology does not actually push a plastic credit card nor someone's checkbook over the wires of the Internet. Rather CyberCash provides software based technology tools which pass secure information over the Internet, the secure information then becomes the functional equivalent of the physical plastic card or of a paper check. The software based technology tools permit the smooth integration of the new "information based" plastic cards or "electronic" checks with the older manual systems.

Credit Cards

For example, as the credit card associations announce standards governing the use of their cards on the Internet, CyberCash creates software which implements these standards. The software includes components which run concurrently on the consumer's personal computer, on the merchants' computers, and at a gateway into the banking systems. CyberCash provides this

software free of charge to the banks and to the credit card associations, who then in turn provide this software to merchants and consumers. The software components then work in unison, transporting credit card information securely to the acquiring bank of the authorized merchant. The acquiring bank, as part of their normal discount rate charged to the merchant, assumes the cost of transporting that transaction through the financial networks, including a fee of a few cents to CyberCash. This is the functional equivalent of the "800" number transport fee which acquiring banks pay today.

Though the physical plastic may be missing in this transaction, there is much more security and privacy in this Internet transaction than exists in the physical world today. In the new Internet transaction, all parties-the consumer, the merchant and the bank-are authenticated using a technology called digital signatures. These digital signatures are many times more secure than any handwritten signature we may use today. The consumer will no longer need to be concerned about losing his credit card. Without the consumer's "digital signature" the credit card number is worthless on the Internet. The consumer can have absolute confidence the merchant is an "authorized merchant" because the software on the consumer's computer has the proof of the bank's digital signature. And of course the bank receives the undeniable digital signature of both the consumer and the merchant.

For privacy all transactions are completely encrypted and absolutely protected from monitoring or tampering of any kind. Thus on the Internet we will achieve simultaneously a dramatically improved level of both security and privacy.

Standing behind these systems is the entire strength of the banks and the credit card associations--effectively the strength of the American banking system. Since the introduction of credit cards, the industry has evolved systems to monitor and control risk, while at the same time providing ever more and varied payment products to the consumer. Competitive pressures have continued to drive costs down and to squeeze risks out of the system.

As we move into the world of credit card use on the Internet, we urge that the competitive pressures which have driven the evolution of the industry to date be trusted and be permitted to continue driving evolution on the Internet.

Electronic Checks

Our checks and checking accounts are even more a part of our lives than are credit cards. To have a checking account you do not have to "qualify" under the rigid credit requirements of the credit card industry. To receive a check from someone else, you do not have to be a "qualified merchant." I often ask my friends in the credit card industry when was the last time they used their Visa or MasterCard to send $10 to their mother. Not recently! So checks are an important part of our economic lives.

As the Internet is, in many ways, making geography evaporate (the whole world exists more or less instantly on the PC screen on your desk), so that same Internet technology will give a whole new utility and dynamism to that old check book in your pocket.

While checks are wonderful, we as a society are fairly well educated that checks also have some problems...generally referred to as an occasional "bounce" or an occasional forged signature.

Well, we have some good news for you. The same software technology tools that are being built to make credit cards safe on the Internet also make checks safe on the Internet. With the speed and instantaneous nature of the Internet, we no longer have to wonder if a check is good...we will know instantly...at the time we accept it. Through the software technology tools that CyberCash is building for the banks, funds will be certified prior to the check being sent. Checks received by you, received within seconds of their being sent, will be literally as good as money in the bank...because that is exactly where the money will be...in the bank.

Also, the same technology of digital signatures and encryption that we use to secure credit cards on the Internet will be used to secure checks. No longer will there be forged signatures. Digital signatures effectively eliminate forgery. No longer will there be false claims of forgery; digital signatures are essentially non-deniable. No longer will there be theft of checks in the mail. Checks will travel over the Internet in totally secure encrypted envelopes.

The automated check clearing system in the United States, in spite of the problems of paper transport, has developed into a surprisingly low cost and efficient system. Most of the traditional banking system is built around the accounting for and managing the flow of paper checks around the country. Regulatory agencies have built systems to in turn ensure the safety of the banking system behind the massive flow of checks.

By enabling checks on the Internet, we are building upon this same foundation. We are leveraging the experience of a hundred years, while simultaneously removing some known problems. Perhaps most importantly, checks represent a personal relationship between the check book holder and his or her bank. In the new world of the Internet, that special relationship of credit, trust and responsibility will be given a new lease on life. And that new lease on life will be due to the technology of the Internet, namely instantaneous transfer of information, digital signatures, and encryption.

In conclusion, we would urge the committee to join us in our optimism in seeing the enhancement of some old payment instruments by the new technology tools. We would further urge the committee to embrace our faith in the ability of competitive market place pressures to continue to bring consumers safer, more convenient and lower cost payment options.

Respectfully submitted,

William N. Melton, CEO
CyberCash, Inc.

STATEMENT OF

ROSALIND L. FISHER

EXECUTIVE VICE PRESIDENT

VISA U.S.A.

before the

SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL MONETARY POLICY

of the

COMMITTEE ON BANKING AND FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

July 25, 1995

THE FUTURE OF THE PAYMENT SYSTEM

Testimony before the Domestic and International Monetary Policy Subcommittee of the House Banking Committee

July 25, 1995

Mister Chairman, Members of the Subcommittee, my name is Rosalind L. Fisher, and I am Executive Vice President of Delivery Systems for Visa U.S.A. I am responsible for the Visa data communications and processing systems infrastructure -- which we call VisaNet. This network is the cornerstone of our current payment system and the foundation on which we are building the new products and services that will be the payment systems of tomorrow. It is an honor for me to speak to you today about that future on behalf of Visa and its more than 19,000 member financial institutions.

Visa is an association that is owned by those institutions. Visa banks issue more than 402 million payment cards, which are accepted at 13 million merchant locations around the world; Visa itself processes more than $630 billion in transactions annually.

While there has been much recent press attention to "electronic money" and the role of a host of new entrants into the business, I am proud to say that Visa and, most importantly, its member financial institutions are playing -- and must continue to play -- a central role in the introduction and use of these electronic consumer payment services. I say "central role" for two different but equally compelling reasons.

First, Visa and its member banks have a solid track record of developing an array of payment systems that meet consumer needs, and we are confident of our ability to continue to do so. Second, the integrity of the payment system, and public confidence in it, could be at risk if so called "electronic money" becomes nothing more than zeros and ones -- digital signals -- without the backing and central involvement of regulated financial institutions.

As to the first point, the success of Visa's products is well known. From our Visa Classic and Visa Gold credit products to business solutions such as the Purchasing Card, the Business Card and the Corporate Card, Visa and its members offer many credit options to consumers and businesses alike. Visa also offers the Visa Check Card, an off-line debit card, and Interlink, an on-line debit card (debit cards access a deposit or share draft account); Visa TravelMoney, a prepaid card for obtaining local currency worldwide at favorable exchange rates; and Visa Travelers Cheques. Visa also runs the largest global ATM network under the "Plus" brand, as well as an automated clearing house service and an electronic check imaging service.

The second reason Visa and its member financial institutions must be involved in these evolving services has a public policy foundation: the integrity of the payment system and public confidence in it demands that regulated financial institutions be central players. While we must ensure such involvement, we caution that premature government regulation -- or the failure to modify existing regulations to accommodate evolving technologies -- could chill or halt the delivery of new financial products to consumers.

I will comment further on this important issue in a moment, but first let me give you a closer look at some of the products and services of the future.

Evolving payment systems is the very core of the Visa mission on behalf of its members. In fact, the Visa organization is itself an example of that evolutionary process. And since the first authorization of the blue, white and gold card over the telephone more than 25 years ago, Visa and its members have been helping to shape that evolution in ways that provide benefits to consumers and merchants around the world.

By providing payment systems that offer consumers and merchants convenience, security and utility, Visa and its members have played a vital role in leading beneficial change in the way business is conducted around the world.

New and innovative technology is the underpinning for the evolution of payment systems. The ability of Visa and its member financial institutions to lead these changes has been enabled by our efforts to harness new technologies and leverage their benefits. While the Visa approach relies on technology, it is consumer and market driven. High tech dazzle only adds value when it provides solutions and products that consumers want and need. Visa and its members build products and services that work for their cardholders and merchants based on innovative technology.

Building solutions that work for consumers and merchants means focusing on much more than just technology -- it means adding value and convenience to their lives and their businesses. It also means adding value while addressing issues of key importance. Questions of security, risk and privacy are all crucial

factors in the development of payment products and services. Does this product offer security to consumers and merchants alike? Will it protect financial institutions and their customers from risk? Does it offer protection of data and privacy for its users? All of these questions must be answered and addressed before you have a business solution. And all of these factors are the crux of the goals of Visa and it members as we move toward the technology-driven payment systems of the future.

Chip technology and stored value cards

One of the key technologies that will move our payment system into the future will be that of the integrated circuit chip. Cards embedded with microprocessor chips are often referred to as "smart cards." The microprocessor can be used to store both financial and non-financial information.

Visa's first application of this chip technology is a stored value card that we call Visa Cash. This card is prepaid with a set amount of value loaded onto the microchip and is an alternative to cash for consumers making small purchases, usually those under $20. Our research shows a huge demand from consumers for this product -- and huge consumer benefits.

Imagine the convenience of parking at the Dunn Loring metro station without having to dig in the glove compartment for change for the meter -- getting your Metro ticket quickly and easily without having to worry about the dollar bill being crinkled and spit back at you and stopping to buy a copy of the *Post* and a bagel downstairs on your way to the office -- all with this one card.

Stored value cards will significantly benefit consumers, merchants and others involved in payment transactions. Consumers will benefit from ease of use, convenience and increased transaction speed compared to cash and checks. The stored value card also will be beneficial to those consumers who don't already have many payment options. A bank account isn't necessary to use a stored value card. This product could provide payment card utility for those consumers who don't have or prefer not to have, a relationship with a financial institution and thus don't have cash readily available through ATMs or the ability to easily cash checks.

Merchants will benefit from reduced costs as a result of less pilferage, theft and vandalism (particularly in unattended and mass transit environments), and reduced cash handling due to electronic payments. They will also benefit from increased transaction speed.

One of the locations that merchants are most excited about is automated locations, such as vending machines. This technology will increase the security of accepting payment at these locations and decrease the costs of dealing with coins and currency.

Visa Cash will be introduced in the Southeast in the Fall of 1995 and showcased during the 1996 Summer Olympics and will be available in disposable and reloadable forms. Reloadable cards allow consumers to put additional value on the card at convenient locations such as ATMs. The card can be a stand-alone -- that is, with only a stored value function -- or the stored-value function can be placed on another card, such as an ATM card.

While stored value is the first application of chip technology available to consumers, others are in development now. The next function likely will be one which allows consumers to utilize the product for the maintenance of loyalty or frequent-buyer programs. Consumers will be able to access frequent-flyer programs, electronic coupons and other buyer-rewards programs quickly and easily through this application of technology.

Remote banking

Not all of the products and services being introduced by Visa and its member institutions are card-based. Electronic or remote banking is one of the most important initiatives in which exploding technology is enabling Visa and its members to build new product offerings that bring great value and benefit to consumers. Remote banking will be a cornerstone of the next generation of the payment system -- and Visa and its members are at the forefront of this burgeoning arena.

To truly benefit consumers, remote banking must first be accessible and easy-to-use. Choices such as the type of access device and user software must be left to the individual to provide usable value. For that reason, Visa's remote banking subsidiary, Visa Interactive, offers or is developing interfaces to almost every access device imaginable. From simple touch tone phones and screen phones to personal computers, personal digital assistants (PDAs) and interactive television, Visa is offering a myriad of options for member financial institutions to present to their customers.

Besides access, Visa is also leveraging the VisaNet system and the latest advances in client server and networking technology to offer an electronic remittance system that for the first time will make bill payment a truly electronic function. The services that today tout "electronic payments" are actually only partially electronic, with checks and other paper being heavily used. In fact, while the customer may transmit the payment order to the bank electronically, today the bank often must forward payment to the payee with a paper check.

The Visa bill payment solution is the first system that connects consumers and merchants electronically and is two-way. By streamlining the process we trim the time necessary to move payments and drastically cut the costs of doing so. Consumers can pay their bills in an on-line direct manner easily and inexpensively. This process could save billers such as utilities, telephone companies, and insurance companies anywhere from 25 to 75 percent of their costs for remittance handling and invoicing. And that could mean enormous savings for consumers and financial institutions.

Electronic Commerce

Remote banking is only one area of on-line services into which Visa and its members are quickly moving. Electronic commerce over open networks such as the Internet is a technology-driven market that is exploding and Visa is working with its members to facilitate this rapidly evolving electronic marketplace.

While many are addressing various aspects of this developing market through exciting technology, Visa is building business solutions to meet this market's needs. Our first initiative in this area is providing security for payments made

over open networks such as the Internet. Regardless of the technology, the real game when transacting business over the Internet is knowing who you're doing business with. The groundbreaking efforts of Visa and its members in working with Microsoft to build a standard for making transactions secure will allow consumers and merchants the confidence and protection they need to use this new commercial arena successfully. This security -- and knowing who you're doing business with -- will be key to the future of our country's payment system.

These products and services are just the tip of the proverbial iceberg. From virtual reality banking to value exchange through infrared beams, exciting new ' possibilities are continuously being explored, supported and developed by Visa and its members.

Regulatory Issues Relating to Future Payment Systems

The products and services I've outlined will be offered by Visa's member institutions, which today are the major providers of payment system services to our nation's consumers. Confidence in those institutions and the payment services they provide is high, and for good reason. They are regulated by the federal financial institution supervisory agencies and are subject to regular examination by these agencies and state supervisors. Customers' funds are protected by the safety net of federal deposit insurance. As a result of these protections, the public has a high degree of confidence in our members and their products and services, which is essential for economic stability and growth.

Some electronic payment services may be offered through entities that are not subject to the same supervision and regulation as Visa's members. Their

customers will not have the protection of the bank supervisory system. Furthermore, to the extent that these entities, as a result of not being regulated by bank supervisors, enjoy a competitive advantage over traditional financial institutions, they may worsen the disintermediation of traditional depositories. For this reason and because of the importance of developing electronic payment systems to the world economy and the importance of preventing abuse in these systems, it is significant to note that a recent report by the European Union's Working Group on EU Payment Systems proposed that only banks be allowed to issue stored value cards.

Visa also believes that providing new payment products and services through regulated and supervised financial institutions ensures significant safeguards that are not otherwise available. As stored value cards become an important medium of exchange, policymakers must be cognizant of the potential economic consequences that would result from a loss of public confidence in major unregulated, uninsured issuers. Law enforcement officials combating criminal activities like tax evasion, counterfeiting and money laundering should consider the potential problems that could result from the development of stored value card systems that, unlike Visa's, may not generate a well-defined audit trail and also could result from systems whose record-keeping is not subject to periodic supervision and examination. Accordingly, Congress should carefully examine the risks that are attendant with participation by these other entities in the payment system.

On the other hand, in view of the highly regulated environment in which our members operate and the numerous safeguards that are already in place with respect to depository institutions, we are concerned that additional regulation in

this area will stifle the innovations that are being developed. Products and services such as those described here are in nascent stages and could be adversely impacted by overregulation. At the extreme, subjecting many of these products to government regulation could result in their premature death.

The potential application of the Electronic Funds Transfer Act and Regulation E to stored value cards is an excellent example of this. Regulation E requires that consumers get receipts for electronic funds transfers, such as ATM transactions. If applied to stored value cards, the product will lose its utility entirely for many of its essential applications. As I noted earlier, one of the most practical applications of the card will be at vending machines, parking meters and other facilities and merchants geared to small dollar transactions. Stored value cards will not be economically viable if machines must be re-engineered to give the user a receipt for a 75 cent soda or 30 minutes at a parking meter.

Also, keeping in mind that one need not have a banking relationship to get a stored value card, that a name and address are not necessary and that value on a card may be used quickly, the periodic statement requirements of Regulation E also would destroy the product's utility. These cards will be available at a variety of locations, including dispensing machines such as those used to dispense Metro fare cards on the D.C. transit system. It simply is not economically feasible to equip these machines to obtain, store and transmit all the personal information needed to comply with the periodic statement requirements of Regulation E.

Moreover, it would be extremely difficult and costly, if not impossible, to develop additional products consumers demand such as electronic bill payment,

other remote banking products, and electronic commerce if their development were stunted by premature and burdensome regulation rather than letting the marketplace shape the new technology.

These are only a few examples of how product development, if shaped by regulation, rather than by market forces, would be stunted. Laws and regulations should not be implemented unless they have been proven to be necessary and they can be implemented without imposing excessive costs and burdens. Other countries have encouraged innovation by letting products take shape without undue interference. In order to encourage development and create an environment in which the U.S. can assume a leadership role in these endeavors, we need to do the same. We urge Congress to avoid adding to the regulatory burden of depository institutions, and permit the public to continue to enjoy the benefits of new products and services that Visa and its members are bringing to market.

Once again, I would like to thank the Members of the Subcommittee for the opportunity to testify.

Coin World July 17, 1995
vol 36 no 1840

Visa poised to replace small notes, coins with chip-based debit cards in United States

Electronic cash may soon be a way of life

By Richard Giedroyc
COIN WORLD Staff

Stored value prepaid debit or "smart cards" will begin replacing coins in circulation sooner than many Americans think.

See related story Page 67

VISA STORED Value Card with $20 storage capacity in its microchip, which is located in the circle at left, will soon be available to be used to make cash purchases of goods and services in the United States.

Visa, the credit card giant, is now preparing prepaid debit cards to be mass marketed in the United States.

Visa TravelMoney cards for carrying cash anywhere in the world and Visa Stored Value Cards are now being prepared for use in the United States. The cards were unveiled March 23 in New York.

Visa is implementing a variety of stored value card pilot programs in selected cities in all five Visa regions: Asia-Pacific, Canada, Europe/Middle East/Africa, Latin America and the United States.

Four U.S. financial institutions will issue the Visa debit card during 1995. Bank of America has already issued cards to Visa employees at Visa international headquarters in California.

The cards used at Visa headquarters have created a form of a test market. The cards have a microcomputer chip and are capable of storing value electronically. They can be loaded from an automatic teller machine (ATM) directly from the cardholder's bank account.

First Union Bank, NationsBank and Wachovia Bank have individually agreed to participate in the Visa pilot for the 1996 Summer Olympics to be held in Atlanta.

Visa has been an Olympic sponsor since 1988 and has been designated as the "Official Card of the Olympics."

Cards previously introduced in the United States by other firms primarily use a magnetic strip to store value or are "remote cards" where someone must telephone a computer to activate credit value stored in that computer that is identified through a pin number on the card. Remote cards have no value physically stored on them.

Visa Corporate Relations spokesman Barbara Kalcus told *Coin World* the Visa Stored Value Cards are used in vending machines at Visa headquarters offices by day and are downloaded to the proper bank account by night when the telephone rates are at their lowest.

According to Visa information supplied by the marketing firm Design One in San Francisco: "From the moment the cards were introduced, employees responded with an overwhelmingly high level of interest and enthusiasm.

"Visa found that many $5 cards were kept by employees for their unique and whimsical qualities, and as a result of the card's convenience and popularity, the $20

Please see **VISA** Page 67

Coin World July 17, 1995
vol 36 no 1840
p2/2

VISA from Page 1

cards sold out much faster than anticipated.

"The pilot program's results gave senior management the needed information to seriously consider introducing Visa Stored Value Cards to their employees worldwide and then ultimately to the general public."

Visa is forming a vendor partnership program with 20 of the world's market leaders in the consumer payments industry to develop terminals and cards designed to support common chip specifications. The goal is inter-operability, where a card can work in any stored value system internationally.

The cards are planned to be usable in laundromats, vending, fast food purchases, grocery and convenience stores, school cafeterias, pay telephones, gas stations, taxies, mass transit, road and toll bridges, parking, newspaper purchases and entry to stadiums and theaters.

According to Design One information, the Visa TravelMoney cards will have graphics of a globe nestled among scroll-like graphics meant to look similar to engravings used on U.S. paper money. Shades of green, gold and blue were chosen "to add warmth while simultaneously communicating a contemporary image."

Design One was asked by Visa to design a $5 commemorative card and a $20 value card. The 3,000-card issue of $5 cards was a gift to Visa employees. The $20 card was made available at Visa headquarters and could be used to make vending machine purchases at that facility. CW

Electronic wallets

An imagined world of 'digital cash'

FT p. 14
FT Review: Information Technology
4/7/95

Mobile computing requires miniaturisation and there is a natural physical limit to how small a computer can be made. After all, a keyboard must be large enough to be comfortable and a screen cannot get too small without becoming unreadable.

But if users dispense with the keyboard, and if they do not need a large display area, mobile computers could one day become electronic wallets. They could store "digital cash," display pictures of family members, carry digital business cards – all the things that people have in their regular wallets, *writes Tom Foremski.*

These wallet PCs might seem fanciful and even slightly ridiculous, but they are a goal of US and European researchers and they could become a realistic option by the end of this decade.

One of the most vocal supporters of the wallet PC idea is Microsoft chairman Bill Gates. At the Comdex/Fall computer show last year, he introduced a film depicting Microsoft's view of the future, specifically how people will be using new technologies in Microsoft's home town of Seattle, ten years from now.

The most striking aspect of this imagined world was that there was no cash, at least not in the familiar physical sense. Purchases were made using small, wallet PCs that used wireless infra-red links to make and receive payments. Paying for a cup of coffee from a street vendor was as simple as pointing the wallet PC as if it were a remote control for a television set and pushing a button. A mother was shown giving her son his weekly pocket money by making a wireless transfer from her wallet PC to his.

With Gates a keen advocate for wallet PCs and with Microsoft's enormous influence on the IT industry, a technology direction has been set that is certain to attract other companies. After all, there is a potential market of hundreds of millions of customers in the US alone, not to mention the billions of people worldwide yearning for their own electronic wallets.

Microsoft is not alone in exploring the idea for wallet PCs. The European Union's Esprit research program has a project called Cafe (Conditional Access for Europe) which is working on design and security issues related to creating an electronic wallet. The Cafe wallet will also use infrared technology for wireless payments and prototypes are being prepared for trials later this year.

To prevent others from stealing digital cash transmissions, Cafe is using public key cryptography technology which makes each payment specific to the recipient. The results of several other Esprit research projects will eventually be included in the Cafe project. These include Cascade (Chip Architecture for Smart Card to your home. The same could happen with watching TV – the capability to instantly buy anything you hear or see.

THE NEW YORK TIMES, MONDAY, JUNE 12, 1995

Microsoft Developing Electronic Cash Card

By SAUL HANSELL

Microsoft's dominant software business often seems like a license to print money. But now the company wants to go a step further and make cash itself, at least the electronic kind.

Microsoft is developing a plan to offer plastic cards embedded with microchips, known as smart cards, that can be used to make payments, said Warren T. Dent, the director of business development for the company's consumer systems division.

"I hope in a year or so we are testing something with a stored-value card," Mr. Dent said. The initial test may be with Microsoft's own employees before the technology is offered more widely, he said.

Microsoft would be entering what has rapidly become a crowded field of companies hoping to become to electronic money what Microsoft is to computer software. In July, two large British banks will begin testing Mondex, a so-called electronic purse card, which stores cash. Mondex is economical for small purchases because merchants would not need a telephone link to a central computer. The card's current value is imprinted on the card, which means losing the card is like losing cash. A debit card, by comparison, is more like an electronic check.

Mastercard International and Visa International are also developing chip cards that can hold cash, as are Bank of America and other banks. Separately, a number of independent companies have started to create schemes for sending payments over the Internet, in which cash is loaded onto computer disks rather than on smart cards.

Microsoft is working with chip manufacturers to develop the specifications of its card, and then expects to approach banks that would stand behind the payments on the card. Executives of several of the country's largest banks say they have been approached by Microsoft.

"No matter how much technology you have, one day someone will outfox you," said Richard Lonergan, executive vice president of Visa. "The bank card systems have the risk-management and early-fraud-detection systems that they don't have."

Microsoft might have difficulty finding partners. It frightened many bankers with its now-aborted plan to acquire Intuit Inc., the maker of Quicken personal finance software, which was seen as an attempt to dominate the market for computerized banking and payments known as electronic commerce. Microsoft's chairman, William T. Gates 3d, did not make any financier friends when he was quoted as calling bankers "dinosaurs."

Last week, Mr. Gates tried to mend fences at a meeting in Seattle of the 100 top executives of the world's largest banks. "I actually said the computer systems of banks are dinosaurs," Mr. Gates said at a news conference after the meeting.

Mr. Gates said Microsoft would develop smart cards, software programs and other programs that would work with banks.

"In no way will we be competition to banks in what we're doing," Mr. Gates said. "We're coming up with ways for banks to use our technology. We will never be in the business of doing what banks do."

Microsoft officials have long expressed a desire to write operating systems and software for computerized devices of all shapes and sizes. The company has already introduced a watch, in conjunction with Timex, that stores telephone numbers and appointments.

Electronic Cash

Digital smart cards look like credit cards, but they have an embedded microchip that can perform a variety of functions. Microsoft is developing a smart-card system that would compete with several others aiming to replace cash with digital money that would be stored on a card and be spent for small purchases.

Unlike today's debit cards, which electronically transfer money from a customer's checking account, the cash value would be digitally stored on the card itself. Retailers would use a smart-card terminal to deduct the amount for each purchase. At least four other organizations are developing such cards, which they plan to begin testing over the next year.

Mondex
START DATE July 1995
Test in Swindon, England, of electronic cash card, backed by two of Britain's largest banks — National Westminster Bank and Midland Bank — with the intention of eventually signing up other banks around the world.

MasterCard
START DATE By end of 1995
Test in Canberra, Australia, of smart card that combines electronic cash with existing credit or debit cards to be issued by four Australian banks.

Visa
START DATE Summer 1996
Test of electronic cash cards at Summer Olympics in Atlanta wit three banks: Nationsbank, First Union and Wachovia.

Electronic Payment Services
START DATE July 1996
Test of Electronic Cash Card in Delaware by MAC Automated Teller Machine network

BANK LETTER

A PUBLICATION OF INSTITUTIONAL INVESTOR, INC.

VOL. XIX NO. 25 JUNE 26, 1995

IN THE NEWS

WASHINGTON

MINT DIRECTOR EYES GOVERNMENT ROLE IN PLASTIC MONEY—TREASURY ON BOARD.

Electronic money—smart cards or "E-cash"—is coming, and U.S. Mint Director Philip Diehl wants the government to think about getting in the game. In an interview with *Bank Letter*, Diehl says he has recommended to the Treasury Department that in phase two of the Clinton Administration's "reinventing government" it take a look at the new kind of money and its implications for the old currency and coin-type money the government makes now. A spokeswoman for Treasury said, "Several parts of Treasury are looking at possible uses of the smart card. The Financial Management Service is spearheading this." Diehl indicates he himself is open to the idea that maybe the U.S. should offer both a smart card and a debit card. Diehl says his suggestion that Treasury, which oversees the Mint, ought to look into these possibilities was well received at the department.

There could be government cards side by side with private-sector smart cards,

(continued on page 9)

MINT DIRECTOR *(continued from page 1)*

Diehl says. Or the feds could be a critical part of private-sector development of the new stored value cards. "We might provide critical mass," he says— "a universal standard for a universal card." Technology for machines accepting the cards could be made uniform everywhere, thereby greatly expanding the marketplace. The problem for issuers of the new smart cards would be how to make them as universally acceptable as today's coins.

Up on Capitol Hill, where the ultimate decisions about coins versus electronic cash will eventually be made, there has been a perceptible shift of interest in recent weeks. The monetary policy subcommittee of House Banking has begun to formulate unannounced plans for a series of hearings, starting July 25, which have been tentatively entitled "The Future of Money." The hearings will examine the implications of electronic cash.

Since the district of the chairman of the subcommittee, Rep. Michael Castle (R-Del.), includes more private-sector card issuers than any other congressional district in the country, the panel is likely to be more interested in how the government can facilitate E-cash than take it over. Castle indicated there is no set agenda for the hearings yet. "We'd like to take a look at the entire spectrum of limitless possibilities that have opened with money," the lawmaker said.

Diehl thinks the new electronic money, a market which several banks and other issuers are wading into, will be a much more fundamental change than the introduction of credit cards. Already, for a decade there have been prepaid cards to pay for single-purpose spending such as on subway trips or phone calls.

But these have been restricted both as to where they could be used and for what purpose. Now in the planning stage, however, is a next generation of stored-value cards with a computer chip inside that it is envisaged will be usable in a variety of locations for a broad range of purchases—E-cash.

"I think it's in Treasury's interest to recognize that electronic forms of cash are inevitable," Diehl says. "And we need to think through what is the federal government's role." A source with a major card issuer argues if "the private sector is ready, willing and able to do it, why have an inefficient government monopoly?"

Diehl concedes there are parochial reasons why the Mint would want to build up business by following the customer for money away from coins and into the electronic future. But he disavows any set agenda. "Maybe there is no appropriate role for the federal government," he says. Even so, he says, there is still something to be gained by exploring the possibilities.

—*Stan Wilson*

STATEMENT OF HEIDI GOFF

ON BEHALF OF MASTERCARD INTERNATIONAL INCORPORATED

BEFORE THE SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL

MONETARY POLICY

OF THE

COMMITTEE ON BANKING AND FINANCIAL SERVICES

ON THE FUTURE OF MONEY

JULY 25, 1995

Mr. Chairman, members of the Subcommittee, my name is Heidi Goff. I am the Senior Vice President for Global Point of Interaction of MasterCard. I thank the Subcommittee for the opportunity to testify on these important issues.

There are many forces for change at work in the payments industry today. Their convergence will shape the options consumers will have to make payments world-wide well into the 21st century. Twenty-five years ago, credit cards in the United States were considered a payment vehicle for the privileged. Today, credit cards are a convenience for the majority of Americans. And, debit cards provide this convenience for people who choose not to use credit. As payment systems evolve, MasterCard continues to work diligently to be thoughtful and understanding of our role in developing services that are secure and provide value to the system participants.

Today, the forces for change include technology advances in communications, integrated circuits, image processing, data storage and artificial intelligence. Telecommunications are faster and more ubiquitous. Integrated circuits are finding their way onto payment cards throughout the world, vastly increasing the ability to provide payment services in a secure manner. In addition to the storefront on main street, merchants have migrated from catalogue and telephone sales, to electronic storefronts on information networks, such as America On-line and Compuserve and on the Internet. Consumers now browse through product images in their homes making purchasing decisions with maximum information and no pressure.

Changing consumer behavior is having a profound effect on how payments are made. Most consumers today are under greater time pressure. Consumer research tells us that time is one of our most highly valued commodities. For the payments business that means giving consumers the services and access they want wherever and whenever they want it.

At the same time, people are becoming increasingly comfortable with technology. More than half of all U.S. households have computers. And as prices come down, those numbers will go up. Just look at the increase in the use of remote delivery methods such as ATMs, cash dispensers and screen telephones. A recent Bank Administration Institute study found that 77 percent of all U.S. households use remote delivery methods to do at least part of their banking. The younger the consumer, the greater the tendency not to go to a teller. Banks are trying to encourage this

shift as well. It is simply more cost-effective. Right now, technology driven transactions account for more than half of all banking transactions -- 31 percent by ATM, 24 percent by telephone, and 2 percent by other means such as remote banking.

As I mentioned, integrated circuit cards are now enabling new payment methodologies such as stored value or pre-paid cards as well as new security measures which will protect consumers from more sophisticated criminals. Integrated circuits and chip cards, interchangeably referred to as smart cards, will improve the way we make payments, and create new value for the consumer and the banking community.

Today's magnetic stripe card technology can store just a few lines of information. However, a smart card, which can store pages worth of information, can support multiple functionalities; in other words, it can be a credit card, a debit card, and a stored value card wrapped into one. It can also store other information, such as frequent flier or loyalty program points, discount coupons, or insurance information. The consumer will decide what information is stored on the card and what functionalities it will contain.

On the merchant side, stored value cards will allow cash-based merchants to accept payments without the expense of maintaining on-line connections to issuers for authorizations. Once the card is validated, the cash value is deducted from the card. And consumers can load more cash onto their cards as needed from an ATM almost anywhere they happen to be. Loyalty programs maintained on chip cards have endless possibilities for merchants to give consumers reduced price or no-cost goods and services instantly at the time of each transaction.

The smart card also can offer consumers greater security. By encoding the card with a personal identification number, a merchant terminal can verify the cardholder without ever going on line. The cardholder simply inputs his or her PIN, the card and terminal interact to authenticate the PIN number using secure cryptology and if the PIN is correct the card is accepted. Through unique card authentication methodologies, the terminal also will validate that the card is authentic, not a counterfeit.

MasterCard, VISA, and Europay have been working together to develop a single global standard for smart cards and the terminals that accept them. We want to be sure that just like today's credit cards, any terminal will be able to

accept any card. Our progress has been impressive. Already specifications for cards and terminals have been developed. In addition, we are scheduled to begin our first microchip application pilot -- a stored value card -- in Australia later this year.

Expanded Networks

While chip technology will add greater flexibility to payment cards, increased connectivity is giving consumers broader acceptance for those cards. As a result, the point of sale -- a physical place defined by the merchant's locations -- is migrating to a "point of interaction" -- a virtual place defined by the consumer's location.

There are two pieces to the connectivity equation -- expanded networks and a growing number of on-line services. By networks, I'm talking about physical connections, rather than services. Three of the most commonly recognized are telephone networks, cable networks and satellite services. Each of these networks offers a potential path for carrying value transactions. Consumers can do their banking by phone -- in some places they can bank on their television screens. The bottom line is that the availability of these expanded networks increases our ability to serve more and more consumers efficiently and effectively.

The Growth of On-Line Services

On-line services are the other half of the equation. While there are more ways to hook in -- there are also more things to hook to. The electronic superhighway is expanding exponentially. Every day new services become available -- and every day the traffic becomes heavier. More than 25,000 merchants in 150 countries are already on the Internet. It also has 20 million users right now. By the year 2000, our estimate is that more than 100 million people around the world will be connected to the Internet. And you can be sure anyone that has anything to sell will be connected to it as well.

One important role for the payments industry will be ensuring that those value transactions are secure. Right now, with few exceptions, if you send your account information across the Internet, you may be leaving yourself vulnerable -- because those transactions are conducted on unsecured lines. Together with others, we have been working to ensure that on-line transactions can be made securely. And by year end, that will be the reality.

Protecting Privacy

We are also acutely aware that many consumers feel that the greater access to information that the smart card and expanded networks create raises concerns about their privacy. Last year, we joined with Yankelovich Partners to assess the privacy concerns of today's consumers. We also looked at the potential for using personal data for more efficiently offering services to consumers who want them, better fraud protection, and improved customer satisfaction. We recognize that if consumers don't trust us to protect their privacy, they're not going to use our products. Bottom line, consumer trust is key to our continued success. We're currently working with our members to develop effective privacy guidelines.

Adding Value

As a payments franchise, we have committed ourselves to adding value -- value as consumers define it: convenience; security; and flexibility. Technology will enable us to fulfill this commitment more fully. Our members will be able to offer to more and more consumers a payments card that fits his or her specific -- and changing -- needs. And that's a good thing.

Going forward, we are dedicating ourselves to the cost-effective implementation of a flexible payments system infrastructure that provides value to consumers throughout society. And by value we mean the broadest range of products and services -- unsurpassed acceptance at all points of interaction -- and top quality customer service and security -- no matter where the cardholder is. To accomplish this goal will require an atmosphere conducive to creativity and variety. In order to achieve this, we recognize the need to work closely with regulators and legislators to create a healthy and accessible payments system that will serve us well in the years to come.

Thank you again for the opportunity to address the Subcommittee. We look forward to working with you to create a future that serves the best interests of both consumers and American financial services firms.

64 Willow Place
P.O. Box 3014
Menlo Park, California 94026-3014

Testimony of Scott D. Cook, Chairman, Intuit Inc.
before the House Banking Subcommittee
on Domestic and International Monetary Policy
July 25, 1995
on the Future of Money and Payment Systems

Mr. Chairman, Mr. Vice Chairman, members of the subcommittee, thank you for the opportunity to speak to you this morning. My name is Scott Cook. I am the co-founder and chairman of Intuit Inc., located in Menlo Park, California.

I'm sure you've all heard the word electronic commerce a lot recently. Some of you may be wondering what Intuit means when we say electronic commerce.

Electronic commerce is no different from regular commerce in that there are many facets to it. For example, dry cleaners and TV stations are both involved in commerce, but in different areas. Intuit is involved in an entirely different part of electronic commerce than some of today's panelists.

For example, some companies are focused on creating new payment systems. Some companies are focused on allowing people to purchase goods electronically. Intuit's focus is different. Our focus is on providing people and small businesses with tools and PC technologies to communicate with existing banks, brokerage and other financial services in new ways that help them make simply smarter financial decisions. We are not creating new kinds of money.

If you know my company at all, you probably know it for our first and flagship product, *Quicken*, which is the world's most widely used personal finance software. In fact, it is the nation's best-selling software application. However, *Quicken* is just one of the products that Intuit makes to try to achieve our goal of improving the financial lives of consumers and small businesses by helping them make better financial decisions. Our other products include:

- *Quicken Financial Planner*, which delivers a personal retirement plan showing each consumer how they should save and invest to successfully fund their retirement. It is the best-selling software of its kind.

- *TurboTax* and *MacIntax*, the nation's best-selling tax preparation software which enable both consumers and small businesses to file their income taxes more accurately and correctly with far less hassle.

- *Parents Guide to Money,* software which helps new parents with the four financial decisions that they face: life insurance, child care, college savings and health insurance.

- *Quicken Mutual Fund Selector*, software which gives consumers unbiased information to decide which of the thousands of mutual funds meet their objectives.

Also for small businesses we make:

- *QuickBooks*, the nation's best selling accounting software, which keeps books and shows a business person his or her financial condition in graphics and plain English.

- *QuickPay,* the nation's best-selling payroll software, which helps businesses do accurate payroll for their employees.

We also proudly export American technology. To date, our products are the best sellers in every country that we have entered.: Germany, the United Kingdom, Canada, Australia, New Zealand and Austria. That means we outsell every competing product, foreign or domestic, in those markets.

Let me demonstrate what I mean by enabling people to make simply smarter financial decisions.

The important financial decisions people make concern their savings, investments, retirement planning, college savings, insurance decisions, buying a home, financing and re-financing that home, and more. These decisions are not new, but they re quite a bit more complex today for many people than they were 30 or 40 years ago.

Let's look at one example, retirement planning. We all know that structural changes in pension and Social Security benefits have moved the burden of funding retirement onto the consumers' shoulders. Yet, when I speak publicly I ask audiences of computer owners if they have a retirement plan in place -- not simply a 401K -- but a plan that will build a nest egg sufficient to see them through retirement. Only about five percent raise their hands. This is a national tragedy in the making.

Millions of working Americans will retire in poverty, not in prosperity unless they put a retirement plan in place in the next few years. Yet only five percent have retirement plans. Why don't they? Because financial planning is too complex for consumers to do unaided. Sometimes, the pros who are supposed to aid people don't always get it right. And a truly unbiased financial adviser is so expensive that only the very rich can afford it. Books are helpful, but they don't give the answer because they are customized to each person's individual needs and circumstances.

We at Intuit are trying to change this. With software we just introduced this spring, called the *Quicken Financial Planner*. It delivers an unbiased retirement plan, personalized to each consumer's specific situation. It costs $39, which makes financial planning available beyond the richest 3 percent of households to any of the 30 percent of American households with a PC. That's a 10-fold expansion in availability.

(Mr. Cook will demonstrate Quicken Financial Planner at this point)

Mr. Chairman, just a few days ago my company announced we're working to further enhance people's ability to make better financial decisions by giving them a communication link to their bank that will deliver financial information in a rich an automatic fashion.

We are working with 17 of the nation's largest and most trusted banks, plus American Express and Smith Barney to connect them electronically to Quicken customers. This service will provide:

- Electronic delivery of bank brochures and marketing information.
- Access to bank statements electronically, in addition to getting them in the mail.
- The ability for customer to electronically ask their bank to transfer funds between accounts, in addition to asking by telephone, by ATM or in person as they do today.
- The ability to pay bills, enhancing a service banks have offered since the early 1980s, in addition to paying bills by check through the mail as they do today.
- The ability to use other Quicken products such as the Quicken Financial Planner without the need to re-enter the same data.

This work is based on a simple premise: customers and financial institutions both seek closer and deeper relationships. I haven't met a banker yet who did not want closer relationships with their customers. Customers want to be able to deal with their bank whenever they want -- over the weekend or nights.

These close relationships are unfortunately difficult to arrange today. Financial institutions are wonderfully automated and their products are essentially electronic products. On the other hand, there is a gulf between that automation and the consumer It is a gulf filled with established methods, such as branches, postage and mail, advertising and people on telephones. These can be costly and all too often impersonal -- as anyone who receives junk mail knows.

What we are doing is to build another method of communication. This will enable the bank customer to be reached, to be served, to be sold in their homes and offices whenever the customer wants -- 24 hours a day, 7 days a week.

The financial institution benefit is initially in cementing relationships with current customers and helping them gain new customers. Longer term, there will be some nice

cost implications. Ultimately the cost of electronic commerce is built on the fundamental cost of silicon and software -- costs that go down over time. Such a trend can only help banks become more competitive in a financial services market that is truly global. That is good news for the American economy and for your constituents, whose taxes guarantee bank deposits.

Keep in mind that electronic commerce has many suppliers and many channels. This will not be something like cable TV or local phone service where there is one supplier and one channel. Instead, this will be like magazines and radio stations, where there are dozens or hundreds of competing entrants. Intuit is not alone. Some of the biggest names in telecommunications and technology have formed alliances to provide competing electronic commerce services.

The last point I'd like to make about the piece of electronic commerce that we are working on is that there are other benefits.

With software like ours, people will achieve their financial goals better than they have achieved them in the past. The reason is they will have more timely, better organized financial information and be able to use other products that will help them make smarter financial decisions. I believe people will avoid some of the problems that they run into in finances. There will be fewer bad debts and fewer personal bankruptcies, a higher savings rate in the United States and simply more confidence that comes as people are empowered with great tools to help make these decisions. That is our mission and what we and our financial institution partners are trying to achieve.

Finally, Mr. Chairman I have not come here today to seek any action. I am here to provide you with information. However, to the extent that you move forward in this area, I would ask you to consider that there are many excellent rules that are in place to protect consumers and ensure a strong financial services industry. Many of those rules were written before a PC was a glimmer in the imagination. Some of them might need to be updated to reflect the advent of the PC and what PC-owning consumers want.

Thank you, Mr. Chairman. I'll be glad to respond to any questions you or other members of the subcommittee may have.

-30-

ISBN 0-16-052055-X